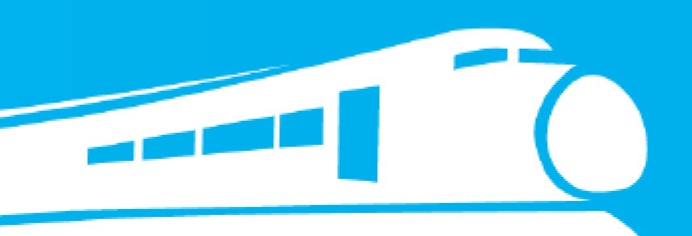
网络工程师
实用培训教程系列

丛书主编 刘晓辉 张运凯 李福亮



网络管理与工具软件应用

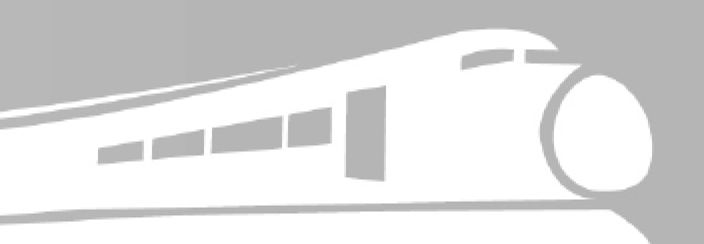
○ 马雪松 褚建立 等编著



清华大学出版社

网络工程师
实用培训教程系列

丛书主编 刘晓辉 张运凯 李福亮



网络管理与工具软件应用

○马雪松 褚建立 等编著

清华大学出版社
北 京

内 容 简 介

本书详细介绍网络管理技术及网络管理工具，并分别介绍了网络服务器的系统管理、网络服务管理、网络设备管理、网络流量管理、网络客户端管理和故障管理等方面的内容。通过简单、易懂的介绍和操作说明，真正使读者掌握书中的知识。另外，在书中还介绍了大量的网络管理工具，通过使用这些管理工具，使管理员能够更加高效地管理网络。本书针对网络管理和监控的实际需求，通过大量的技能特训和综合特训，迅速培养和提高读者的动手能力和技术水平。

本书既可作为培养21世纪计算机网络系统集成工程师的教材，同时也是从事计算机网络的规划、设计、管理和应用集成的专业技术人员的必备工具书。

图书在版编目(CIP)数据

网络管理与工具软件应用/马雪松，褚建立等编著. —北京：清华大学出版社，2010.7
(网络工程师实用培训教程系列)
ISBN 978-7-302-22470-9

Ⅰ. ①网…　Ⅱ. ①马…②褚…　Ⅲ. ①计算机网络—管理—技术培训—教材　Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2010)第067001号

(2014.1重印)

责任编辑：孟毅新
责任校对：刘　静
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京中献拓方科技发展有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：30.75　　**字　　数**：746千字
版　　次：2010年7月第1版　　**印　　次**：2014年1月第3次印刷
印　　数：4001～4200
定　　价：49.00元

产品编号：034324-01

丛书序

PREFACE

近年来，计算机网络在我国已经得到了较快的发展。许多企业、事业单位、行政机关、司法机构和金融系统构建了高速的办公专用网。各种类型的计算机网络高达数十万个，计算机网络已经深入到我们工作、生活和学习的方方面面。

毫无疑问，大量的网络必然需要大量的网络管理人才。初步估计，到目前为止，仅我国每年需要的网络管理人才就达十余万人。随着网络应用的日益深入以及网络所承载的业务量和数据量的不断增长，网络的重要性和安全性也将与日俱增，对网络管理人员的需求也将随之不断地增长。由此可见，网络管理是一个稳定且前途远大的职业。

综观现有的网络技术培养教材，大多将网络技术进行条块分割，按章节、分模块独立讲授，人为地将紧密联系在一起的各种理论和技术分裂开来。这样所带来的问题就是，学生必须将所学的知识和理论全部融会贯通之后，才能初步掌握作为一个网络技术人员所必须具备的一些基本技能，显然这不符合学生的学习规律，也不符合现实的网络管理实际，同时，也是导致许多网络爱好者望而却步的重要原因。

本丛书具有以下特点。

(1) 案例贯穿。本丛书从最常见、最典型的网络应用情境和需求入手，围绕统一的网络环境、统一的网络规划、统一的网络拓扑、统一的资源分配、统一的网络用户和统一的网络需求，提供全面的网络解决方案，以及实用、够用的网络技术，为网络，工程师提供宝典级别的现场技术手册。

(2) 项目驱动。本丛书由情境导入需求，以项目进行教学，再由实训实现强化，进而达到培养技能的目的，最终使学生顺利就业。按照网络构建的工作过程系统化课程开发，以真实的网络管理过程为导向规划课程内容，使读者能够真正掌握网络构建与管理的知识和技能，独立完成相关的网络技术项目。

(3) 贴近实战。本丛书突出“先做后学，边做边学”的主旨，通过“练中求学、学中求练、练学结合、边练边学”的教学内容安排，实现“学得会，用得上”的最终目的。由于全书围绕统一的典型网络工程展开，因此，读者能够非常方便地将教学案例移植到真实的网络项目中，学为所用，学以致用。

(4) 内容全面。本丛书涵盖了作为初、中级网络管理员必须掌握的所有理论和技术，以网络管理的实际需求为导向，以培养基本技能为目的，将枯燥的理论融于实际操作中，从而使学生学得会、记得住、用得上。

(5) 兴趣教学。本丛书设计的教学内容按照“案例情景→需求分析→解决方案→技术操作→理论背景”的结构进行组织，有实际案例、有动手操作、有理论分

析，可以激发读者的学习兴趣和学习的主动性，培养读者解决实际问题的能力，提高读者的综合实战水平。

（6）注重动手。本丛书加大了动手操作的比重，减弱了理论知识的介绍，以适应特定的读者群，体现“做中学”的宗旨。借助大量的网络实验，可以使读者迅速提高技术和技能。

（7）涵盖认证。本丛书充分考虑到了网络管理员的职业需求及职业资格认证要求，在内容安排和习题设置上与相关认证紧密结合，基本涵盖了国内认证（网络管理员、网络工程师）和国际认证（MCSE、CCNA）所涉及的理论和知识技能，以帮助学生获取“双证书”——学历证书和职业资格证书，增强学生的就业竞争力。

（8）资深作者。本丛书作者全部来源于网络教学、网络管理和网络工程第一线，具有非常丰富的网络设计、施工和管理经验，既掌握理论技术，又通晓实际操作。作者们做了大量的技术需求和人才需求调研，多次修改提纲以使其更加符合网络搭建和管理实际。

（9）深度支持。本丛书不仅提供优秀的纸质教材，还为教师提供了电子课件和全方位的技术支持，同时设置有 QQ 群在线答疑、E-mail 离线交流和 BBS 论坛互动平台，并为读者提供网络构建方案和配置技术咨询，形成一个让师生更加方便、更加自主学习的教学环境，有效地提升了教师授课和学生学习的能力。

本丛书删繁就简，围绕一个典型的网络工程展开理论和技术讲解，囊括了网络布线、网络搭建、网络管理、网络服务、网络安全、数据存储等各种组网、管网和用网技术。因此，读者学完本套丛书后，可以直接将其应用至自己的工作实践。即使是初学者，只要熟悉 Windows 的一般操作，就能非常容易地上手，迅速成长为一名合格的网络管理员。

刘晓辉

2010 年 6 月

前言

FOREWORD

随着信息化进程的推进，几乎所有的企事业单位都有自己的网络，而由此产生的网络管理人才的需求缺口正在逐年扩大。据相关部门统计，2009 年网络管理人才缺口达到 13.5 万人，许多企业不惜重金，招募一名出色的网络管理人员。随着网络应用的不断拓展，企业发展对计算机网络的依赖性将越来越强，而掌握大量精尖网络技术的人才也会变得越来越受欢迎。为什么在如此光明的就业形势下，却经常听到网络管理员的工资只有几百元呢？原因很简单，企业真正需要的网络管理员，是能够独当一面、不需不断培训的专业人员。向网络工程师晋升，是摆在网络管理员面前的唯一出路。

本套丛书作为网络工程师培训教材，以实际的公司网络为案例，以打造实用的网络工程师为目标，以实用和技能为主，摒弃了复杂的原理，以简明的操作为引导，通俗易懂，上手容易。读者只需按照书中的操作来学习，就能掌握相应的技能，学完全套书之后，即可掌握大部分的网络知识。

本书以目前中小型网络为管理背景，充分考虑了网络管理所包含的各方面内容，以及网络管理过程中可能遇到的问题，是一本实用性很强的丛书。本书所介绍的所有管理工具及软件均无须掌握复杂和高深的理论知识，或丰富的网络管理经验，只需按照书中操作步骤操作，即可轻松实现网络管理。

全书共分为 13 章，详细介绍管理 Windows 服务器和客户端，Cisco 网络设备的软件的功能、特点及应用实例，网络故障的诊断与排除等方面的知识。第 1 章网络管理规划，从整个网络的管理任务出发，对整个网络项目的管理需求进行分析和规划。第 2 章 Windows 系统管理，详细介绍 Windows 系统管理的内容及方法。第 3 章 Windows 系统性能管理，详细介绍影响系统性能的原因，以及提高性能的方法措施。第 4 章 Windows 系统安全管理，详细介绍提高 Windows 系统安全的方法，以及如何使用系统日志功能。第 5 章 Windows 网络服务管理，详细介绍 Windows 服务的管理方法，以及 Windows 群集技术。第 6 章网络设备管理，介绍 Cisco 网络设备的管理方式，以及设备的配置管理内容。第 7 章网络流量和流量监控与分析，介绍常用的网络性能测试工具、网络带宽测试工具和网络流量统计工具。第 8 章网络链路管理，分别介绍物理链路和逻辑链路测试工具的使用方法。第 9 章网络协议和资源管理，介绍网络协议管理工具和如何管理共享资源等内容。第 10 章网络安全管理，介绍网络设备的安全管理、网络安全设备的管理及客户端计算机的安全管理。第 11 章网络客户端管理，介绍关于客户端计算机的系统更新管理、网络接入管理、组策略管理及使用组策略分发系统和应用程序管理等内容。第 12 章系统故障诊断与排除，详细介绍当系统发生故障时的应对方法。

第 13 章网络设备故障的诊断与排除，详细介绍发生网络故障的原因及排除过程等内容。

为了让读者更深入地了解所学的知识，在每章的最后还配备了习题和实验，从而可以起到复习和测验的作用，能使读者尽快迈向网络工程师的行列。

本书可作为大中专院校计算机网络专业的教材，也可作为中小型网络管理员、网络工程技术人员和网络爱好者的参考书。

本丛书由刘晓辉、张运凯、李福亮主编。本书由马雪松、褚建立等编著，具体分工如下：马雪松编写了第 1～4 章，褚建立编写了第 5～7 章，肖丽芳编写了第 8～9 章，李利军编写了第 10 章，李福亮编写了第 11～12 章，陈志成编写了第 13 章。编者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，本书作为对一段工作的总结与回顾，希望能对大家的系统维护和网络管理工作有所帮助。

由于编者水平有限，书中难免有不足之处，恳请广大读者批评指正。

编　者

2010 年 4 月

CONTENTS 目录

第 1 章 chapter 1

网络管理规划

全面管理网络是网络高效运行的前提和保障，管理的对象不仅指网络链路的畅通、服务器的正常运行等硬因素，更包括网络应用、数据流转等软因素。网络管理者必须时刻关注本企业网络的运行，关心企业对网络的应用，让网络能够随时满足企业的需求，或者说是引导企业的发展。

1.1 项目背景

某高新产品研发企业拥有员工 2000 余人，公司总部坐落在省会城市高新技术开发区，拥有 4 个生产车间和两栋职工宿舍楼，产品展示、技术开发与企业办公均在智能大厦中进行。该企业在外地另开设有两家分公司，由总公司进行统一管理和部署。目前，该企业网络的拓扑结构如图 1-1 所示，基本情况如下。

（1）在当前网络中，所有的网络设备使用的均为 Cisco 的产品，接入层交换机为 Cisco Catalyst 2960，汇聚层交换机为 Cisco Catalyst 3750，核心层交换机为 Cisco Catalyst 4506，防火墙为 Cisco ASA 5540。

（2）服务器所使用的操作系统平台为 Windows Server 2003 和 Windows Server 2008，其中以 Windows Server 2008 为主。

（3）接入 Internet 方式采用 100M 光纤方式。现有接入用户数量为 500 个，客户端均使用私有 IP 地址，通过路由器地址转换接入 Internet。部分服务器 IP 地址为共有 IP 地址。

（4）局域网覆盖整个厂区，中心机房位于智能大厦的第 3 层（共 15 层），职工宿舍楼和生产车间均有网络覆盖。

（5）客户端操作系统采用 Windows XP Professional 和 Windows Vista，其中以 Windows XP Professional 操作系统为主。除部分客户端需要连接 Internet 外，其他客户端均只在局域网内通信使用。

（6）会议室、产品展示大厅等公共场所部署无线接入点，实现随时随地无线漫游接入。

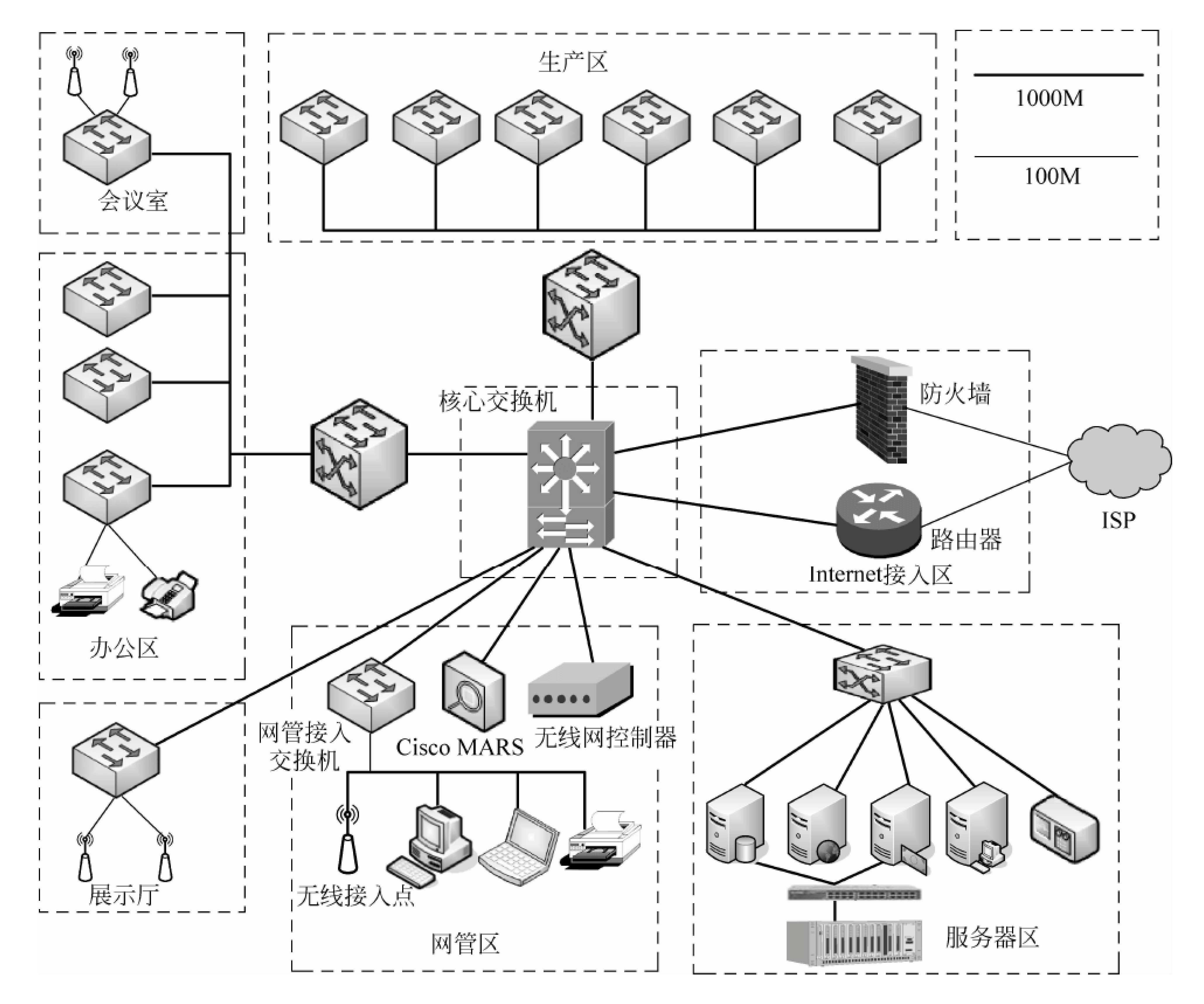


图 1-1　网络拓扑结构

1.2　项目需求

随着企业的日益发展，网络也在不断地发展，随之网络管理的难度也在提高。因为企业只有为数不多的几个管理员，并且各管理员之间的分工不同，即每个管理员分别管理网络的不同部分。因此，更加合理地、统一地管理网络也是管理任务所必需的。

针对当前网络的管理，具有如下需求。

（1）服务器管理需求。因为服务器特殊性的原因，对服务器的管理必须由专人负责，从而保证其正常、安全地工作。作为管理任务之一，管理员还应时时关注服务器的运行状况。

（2）网络设备管理需求。网络设备是网络通信的神经中枢，任何一个设备发生故障，对于与之相关的计算机而言都是致命的。

（3）客户端管理需求。客户端计算机是网络的主要组成部分，用户所有的需求都需要通过客户端实现。另外，由于多数客户端计算机的使用者都无法像管理员般注重计算机的安全，所以客户端的安全性也是不容忽视的。

（4）网络管理需求。只有将计算机接入网络，才能真正地发挥网络的作用，对于网络的管理包括网络链路、网络协议和资源等。

（5）网络安全管理需求。网络安全是每个管理员所必须面对的问题，安全问题也是最

难管理的工作之一。

(6) 故障管理。无论是硬件还是软件都不可能保证永远不出问题,任何一种设备或网络的组成部分都有发生故障的可能。

1.3　项目分析

通过对各部分的管理分析,可以清楚地了解各部分所需要的管理内容。针对于当前网络的项目需求,具体分析如下。

(1) 服务器管理。因为服务器的管理所涉及的内容比较多,从而也使服务器的管理难度比较大。通常情况下,服务器的管理包括如下几方面内容:Windows 系统管理、Windows 系统性能管理、Windows 系统安全管理和 Windows 网络服务管理等。

(2) 网络设备管理。网络设备的管理不单单是设备硬件的管理,软件的管理同样重要。通常情况下,网络设备软件是网络实现各种功能的基础,例如 VLAN 技术的使用。在设备购买后,均需根据网络的需要,进行相关的配置。对于已经可以正常使用的设备,则需要将其配置文件进行备份,在设备软件发生故障时,使用该备份文件进行恢复。

(3) 客户端管理。对于客户端的管理,如果需要实现统一管理的目的,则需要将客户端加入到企业域中,然后再进行相应的管理。

(4) 网络管理。网络管理包括网络链路的管理、网络流量及监控与分析两部分内容,只要网络中的计算机进行通信,就会在网络中产生流量,其中还可能会存在不允许的流量,因此,如果不对网络流量进行管理,其混乱程度是可想而知的。

(5) 网络安全管理。网络安全由多个部分组成,包括 Windows 系统安全管理、网络设备安全管理、网络安全管理、客户端安全管理等。

(6) 故障管理。正如 1.2 节所说,故障的发生是不可避免的,如何才能将因为故障而造成的损失降到最小,才是最为重要的。网络中的故障主要分为服务器故障和网络设备故障,其中服务器故障主要是系统故障。

1.4　项目规划

通过 1.3 节对网络项目的分析,可以对网络的不同组成部分进行相关的管理规划,使管理员的管理工作更加有秩序,使管理员的管理效率更高。

1.4.1　服务器管理规划

根据对本项目服务器管理的分析,服务器管理分为如下几部分内容。

1. Windows 系统管理

Windows 系统管理主要是管理与系统运行相关的内容,其中包括磁盘和分区管理、系统服务管理、网络服务管理、进程管理、任务管理、用户管理、网络配置与协议管理、远程管理等。

2. Windows 系统性能管理

Windows 系统性能管理的目的是保证服务器的性能或提高服务器的性能,使服务器可

以更好地提供服务。为了提高服务器的性能,首先应选择合适的操作系统软件,其中Windows Server 2008 Server Core操作系统是Windows Server 2008系列操作系统中占用资源相对较少的服务器操作系统。其次,对于安装图形界面的操作系统,应关闭不需要的图形化特效,以提高服务器的性能。最后,作为管理员还应随时关注服务器的运行情况,使用可靠性和性能监视器,可以随时监控服务器的性能和可靠性指数。

3. Windows系统安全管理

Windows Server 2008提供了一系列新的和改进的安全技术,这些技术增强了对操作系统的保护,为企业的运营和发展奠定了坚实的基础。使用安全配置向导,可以通过向导的方式增强系统的安全性。通过配置服务器的本地安全策略,从而提高本地计算机的安全级别。

另外,在Windows Server 2008系统中,日志系统是一个非常重要的功能组成部分。通过“事件查看器”中的事件日志,可以收集关于硬件、软件和系统问题的信息。

4. Windows网络服务管理

服务器的作用是为网络提供所需的服务,该功能的实现需要在服务器上安装相应的角色服务,只有安装了相应的角色服务后,服务器才能够为网络提供相应的服务。在Windows Server 2008操作系统中,服务器角色及角色服务的安装都可以在“服务器管理器”窗口中实现。对于服务器角色的管理,则可以通过不同的服务器角色提供的独立管理单元,或在MMC控制台中统一管理。对网络服务稳定性要求较高的服务,则可以通过故障转移群集技术实现,例如文件服务器。网络访问量比较大的服务,则可以通过网络负载平衡技术实现,例如Web服务器。

另外,网络服务的日常监控也是不容忽视的工作之一,这部分工作可以在网络中部署网络服务监控软件,使其7×24小时监控服务器。

1.4.2 网络设备管理规划

网络设备主要是指交换机、路由器和防火墙,这些设备都是网络运行所必不可少的,缺少任何一部分都无法完成正常的网络要求。

1. 管理方式的选择

虽然网络设备拥有自己的操作系统,但却不像真正的计算机一样拥有输入/输出设备,即网络设备的管理需要借助计算机来实现。通常情况下,管理网络设备的方式包括如下几种:超级终端方式、Telnet方式、Web方式和网络管理软件方式。

2. 网络设备的初始化配置

任何网络设备在出厂前,生产商都已经对网络设备进行简单配置,这些配置是达不到用户的使用需求的,例如,无论使用的是何种级别的交换机,如果用户不进行任何配置都只能被用作二层交换机。

3. 配置文件的管理

通常情况下,在网络设备配置完成后,是不会发生改变的,根据管理员的日常工作原则,需要将所有的配置文件进行备份。另外,由于配置文件可以上传到其他设备运行,所以通过备份配置文件,还可以防止在设备发生故障时,使用该设备取代当前设备。需要注意的是,并不是所有的配置文件都是通用的,只能是相同厂商的设备才能实现该功能,这里所指的设

备均为 Cisco 厂商的网络设备。

4. 网络管理软件

使用网络管理软件,可以减少管理员的管理任务,因为管理软件所使用的都是图形化管理,与使用超级终端和 Telnet 方式相比要简单得多。最主要的原因是使用网络管理软件可以很直观地查看网络设备的监控结果。

1.4.3 网络流量管理规划

网络流量是网络必不可少的组成部分,但如果网络中存在大量的非法数据时,则会降低网络的稳定性,此时,则需要管理员了解网络中流量的具体情况,并采取相应的措施。

1. 网络带宽的监控与分析

网络带宽会在网络的使用过程中出现老化现象,当老化比较严重时,同样会影响网络的正常运行,即在网络使用中管理员非常有必要定期对网络带宽进行测试。同样,受外界环境影响较大的无线网络也应进行必要的监控和分析。

2. 网络流量的监控与分析

当网络中存在大量的流量时,会直接降低网络设备的性能,并导致整个网络的性能下降。例如网络中存在使用 P2P 软件的用户等。为了杜绝这种情况的发生,管理员需要实时监控网络流量情况,当网络性能突然下降时,则可以第一时间查看是否是由网络流量过大所引起的,并采取相应的应对措施。

3. 网络吞吐量分析

吞吐量是指在没有帧丢失的情况下,设备能够接受的最大速率。在测试中以一定速率发送一定数量的帧,并计算待测设备传输的帧,如果发送的帧与接收的帧数量相等,那么就将发送速率提高并重新测试;如果接收帧少于发送帧则降低发送速率重新测试,直至得出最终结果。在实际操作中,这些操作均是由软件后台操作完成,管理员只需进行测试前的设置,以及查看测试结果。

1.4.4 网络链路管理规划

常用的网络链路包括双绞线、光纤和电磁波,在当前网络中,除布线困难的地域,其他链路均采用双绞线或光纤。当网络链路发生故障时,可以通过测试工具分别对物理链路和逻辑链路进行测试。

1. 网络物理链路测试

物理链路的测试,通常需要借助于物理链路测试工具,双绞线链路的测试可以使用 Fluke MircoScanner^2 或简易网络测试仪等。而光纤链路的测试,则可以通过光纤链路测试工具。

2. 网络逻辑链路管理

网络逻辑链路的测试,则可以使用 Windows 自带的工具进行测试。Windows 自带的工具包括 IP 网络连通性测试工具(Ping)、路径信息提示工具(Pathping)和测试网络路由路径工具(Tracert)。

1.4.5 网络安全管理规划

当前计算机网络是充满恶意攻击者的网络,恶意软件使用与 E-mail、文件传输、Web 访问和实时合作之间的无缝通信相同的计算机网络技术,进而针对计算机弱点进行攻击。

1. 网络设备安全

正如 1.2 节所述，网络设备是网络的中枢神经，保证网络设备的安全也是保证网络安全的重要组成部分。通常情况下，网络设备的安全需要通过设备的配置完成，例如配置交换机的保护端口、流控制，在路由器上配置 IP 访问列表、MAC 访问列表等。

2. 网络安全设备

随着用户信息安全意识的逐渐加强，安全设备也越来越受到人们的重视，不过，简单的防火墙已难以满足基本安全防御需求。网络安全设备的目的并不是用来挽救或保护已经受到入侵的用户，而是防患于未然，最大限度地避免可能发生的安全侵害。常用的 Cisco 安全设备包括网络防火墙、入侵检测系统和入侵防御系统，这些设备分布在网络中的不同位置，可以为整个网络或重点对象提供更可靠的保护。

3. 客户端安全

对网络客户端进行必要的甚至是严格的安全控制和管理是保障网络正常、高效、安全运行的重要措施。在局域网环境中，普通客户端计算机的安全设置包括锁定计算机、设置高强度密码、配置 Windows 防火墙和启用系统更新等内容。

1.4.6 客户端管理规划

客户端是用户使用网络的基础，只有在保证客户端正常运行的前提下，用户才能更高效地完成日常工作。为了保证客户端的安全，可以从以下几方面内容进行操作。

1. 系统更新管理

Windows 系统漏洞可谓屡见不鲜、层出不穷，而且其危险性和危害性也是越来越大。因此，及时更新系统补丁、修补系统漏洞，保证 Windows 系统安全，就成为网络管理人员的当务之急。

2. 网络接入管理

接入网络的方式包括有线接入和无线接入，使用有线接入方式，即使用双绞线或光纤，直接将线缆的两端分别接入交换机和客户端的网卡即可。而对于无线网络接入方式，则因所用的无线网卡不同，配置方法也有所不同，通常可使用 Windows 配置程序和所使用无线网卡提供的配置程序进行配置。

3. 组策略管理

组策略(Group Policy，GP)是系统管理员为计算机和用户定义的，用来控制应用程序、系统设置和管理模板的一种机制。在当前网络中，首先，可以通过组策略定制客户端的用户环境，从而使所配置的用户使用相同的用户环境。其次，通过配置组策略，限制客户端计算机所使用的硬件。另外，使用组策略还可以在客户端计算机上部署软件，从而减少管理员为客户端安装软件的工作。

1.4.7 故障管理规划

发生故障的概率虽然可以通过管理员在日常工作中降低，却不能完全防止故障的发生。因此，如何在故障发生时及时发现故障并解决故障才是故障管理中的重点。

1. 系统故障诊断与排除

Windows Server Backup 是 Windows Server 2008 的备份与恢复组件。备份与恢复是保证信息系统安全可靠不可或缺的基础。对信息系统来说，可靠性和可用性是最基本的要求。另外，Windows Server Backup 支持图形模式和命令行模式，对于域控制器的备份而言，既可以支持域控制器完整备份，同时也可以支持组件备份。

2. 网络设备故障的诊断与排除

网络故障是一件令人头痛而又不得不面对的难题。对于局域网络而言，网络故障大致可以分为 4 类，即链路故障、配置故障、协议故障和服务器故障。链路故障通常是由于接插件松动或设备硬件损坏所致，而其他故障则往往由人为的设置所致。

第 2 章 chapter 2

Windows 系统管理

Windows Server 2008 是微软推出的强大、安全、易用的网络操作系统。不仅继承了 Windows Server 2003 的安全性、可管理性和可靠性，而且还融合了易用性、人性化、智能化，并在此基础上提供了更丰富的功能和更稳定的内核，非常适合于中小型网络中的各种网络服务，尤其适合那些没有经过专业培训的非专业管理人员使用。

2.1 Windows 系统管理规划

Windows 系统是实现所有功能的基础，无论是网络功能还是本地功能，这也是为什么必须保证 Windows 系统正常工作的原因。

2.1.1 项目背景

在当前网络中，几乎所有计算机使用的操作系统均为 Windows 操作系统，其中服务器主要使用两种操作系统，分别为 Windows Server 2003 和 Windows Server 2008。为使网络用户可以在服务器上存储某些数据，所有服务器均安装有多块硬盘及 RAID 卡。对于服务器操作系统，除拥有多个系统服务外，还包括多个网络服务，因此对服务器服务的管理不仅要管理系统服务还要管理网络服务。进程是服务器当前正在计算的内容，当进程过多时，会影响服务器的整体性能，因此需要关闭不必要的进程。

2.1.2 项目需求

对于 Windows 系统管理需要完成以下要求。

(1) 在网络中，除专用的存储设备外，服务器通常也会承担部分数据存储任务。对于这些数据，则同样需要保证其安全与稳定。

(2) 默认情况下安装的系统服务，可能并不适用于当前的网络。

(3) 对于网络服务的管理，在当前网络中要求实现统一管理的目的。

(4) 每一个服务器运行的程序都会创建一个或多个进程，并通过这些进程实现所需的功能，因此，对进程的管理在系统管理过程中也是不可或缺的。

(5) 对于某些特定的任务，需要在特定的时间自动完成。

(6) 用户和组管理是网络的重要组成部分，需要管理员严格管理网络中的用户和组。

(7) IP 地址和网络连接是服务器连接网络的基础，正确的配置是确保其正常接入网络

的基础。

(8) 对于服务器管理而言，通常会部署在网络中的特定位置。

2.1.3　解决方案

针对当前项目的 Windows 系统管理要求，可通过如下方式实现。

(1) 为了实现服务器存储的安全性和稳定性，可以在服务器安装 RAID 卡，使用 RAID 技术来实现。对于需要在服务器上存储数据的用户，为了防止用户无休止地使用硬盘空间，可以通过设置磁盘配额来实现。

(2) 对于不是系统所必需的服务，通常情况下需要停止其运行。对于系统服务的启动与停止可以通过命令行和 MMC 控制台这两种方法实现。

(3) 对于统一管理网络服务的要求，可以通过在加入域中的计算机上使用 MMC 控制台实现，在 MMC 控制台添加多个想要管理的网络服务管理组件即可。

(4) 对进程的管理主要包括查看进程并将无用的进程和所怀疑的非法进程结束，该工作可以通过 tasklist 和 taskkill 命令实现。

(5) 当在网络中需要在指定时间完成特定的任务时，可以通过 Windows 系统提供的任务计划功能实现。

(6) 用户和组的管理需要根据网络与企业的实际需求进行，通常情况下，为了便于管理需要将用户添加到不同的组中，并对组进行权限设置。

(7) 网络连接的管理主要是服务器的 IP 地址管理和接入网络的方式管理，通常情况下，服务器都会接入固定的网络中，并使用固定的 IP 地址信息。当服务器使用拨号方式连接网络时，则还应创建所需的网络连接。

(8) 对于服务器的管理不会每次均要实现与服务器的面对面管理，通常可采用远程管理的方式实现。

2.2　磁盘和分区管理

在 Windows 操作系统中，数据都保存在磁盘中，并以分区或卷的形式作为目录结构的顶级。另外，为了提高数据的读取速度和保证数据的安全，服务器磁盘通常还会使用 RAID 技术，针对于不同的环境要求所使用的 RAID 类型也有所不同。

2.2.1　RAID 卡管理

一般情况下借助 RAID 控制卡实现硬 RAID，而如果资金不足，则可借助操作系统来实现软 RAID。这里以 Dell PowerEdge 2650 为例介绍 RAID 卡的设置，不同 RAID 卡的设置方式有所区别，请注意查看 RAID 卡的使用手册。

(1) 打开计算机电源，当显示图 2-1 所示的信息时，按 Ctrl+M 键，进入 RAID 卡设置界面。

(2) 使用方向键，依次选择 Configure→Easy Configuration 选项，如图 2-2 所示，并按 Enter 键，实现 RAID 卡的快速配置。

注意：如果该计算机以前配置有 RAID，那么，在配置新的 RAID 之前，应当先使用 Clear Configuration 命令删除。RAID 删除后，硬盘中保存的所有数据将全部丢失。



图 2-1 提示 RAID 卡设置组合键

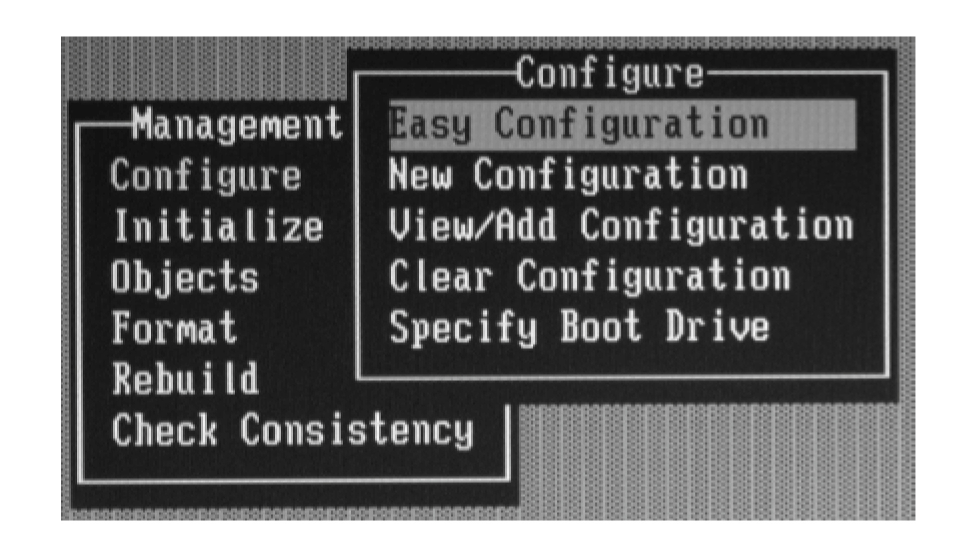


图 2-2 采用 Easy Configuration 方式

(3) RAID 卡搜索并显示该计算机中安装的所有硬盘驱动器,如图 2-3 所示。

(4) 使用方向键选择欲添加至 RAID 的磁盘,然后,按空格键选中,将该硬盘添加至 RAID 阵列,如图 2-4 所示。

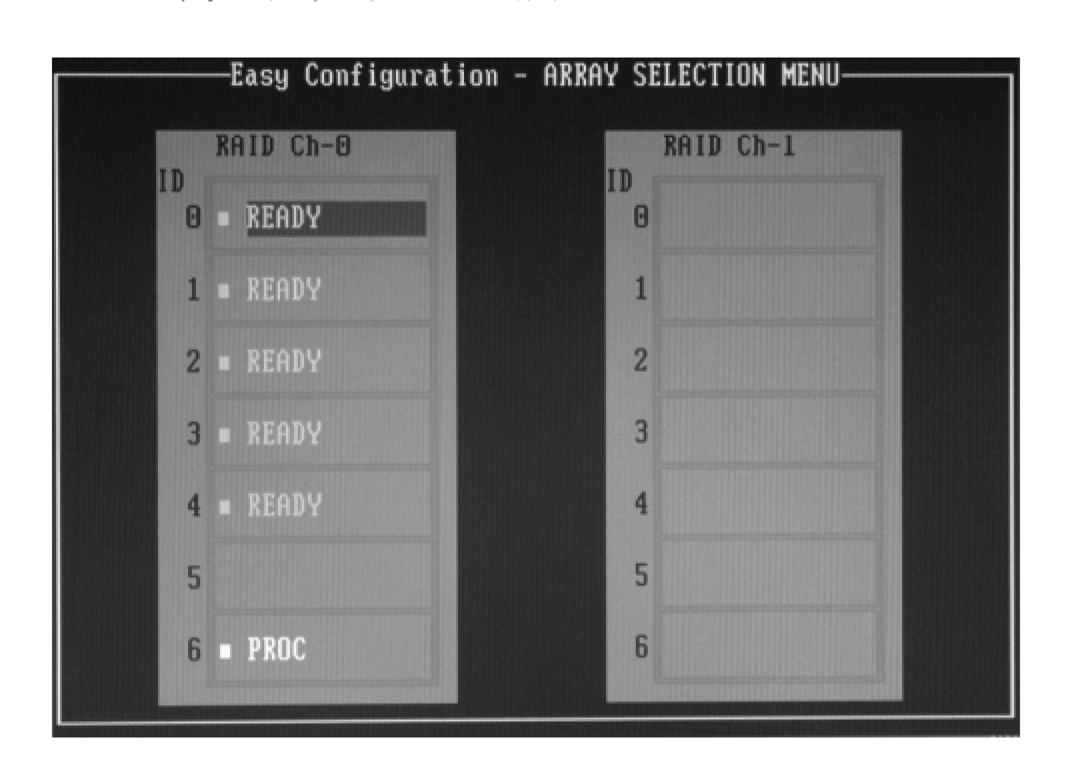


图 2-3 显示所有的硬盘驱动器

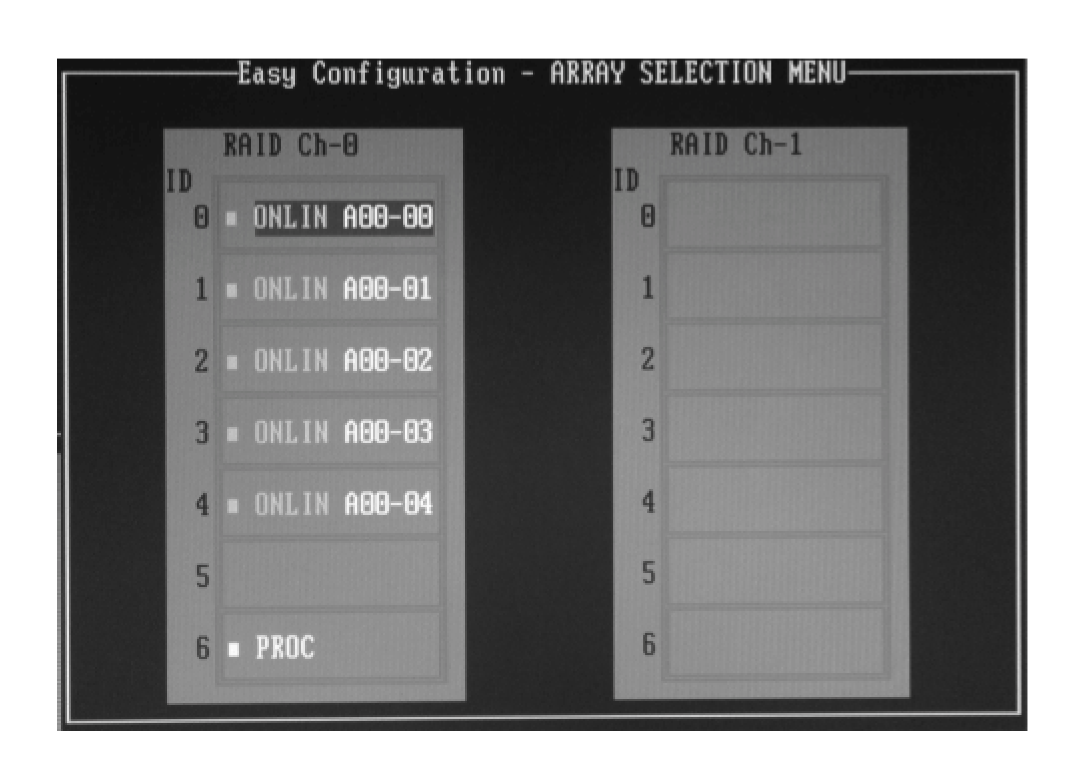


图 2-4 选择欲添加至 RAID 的磁盘

注意:*若欲设置 RAID 5,为了最大限度地提高磁盘空间利用率,应当将所有的磁盘都加入至 RAID。若欲设置 RAID 1,则需要添加两块硬盘。*

(5) 按 Enter 键,显示图 2-5 所示的页面,使用方向键移动光标选择欲配置的阵列。如果只使用了一个通道,那么,应当选择 Span-1 选项。

(6) 按 F10 键,显示图 2-6 所示的页面,选择欲使用的 RAID 级别。当计算机安装有 3 块以上硬盘时,系统默认的级别为 RAID 5。

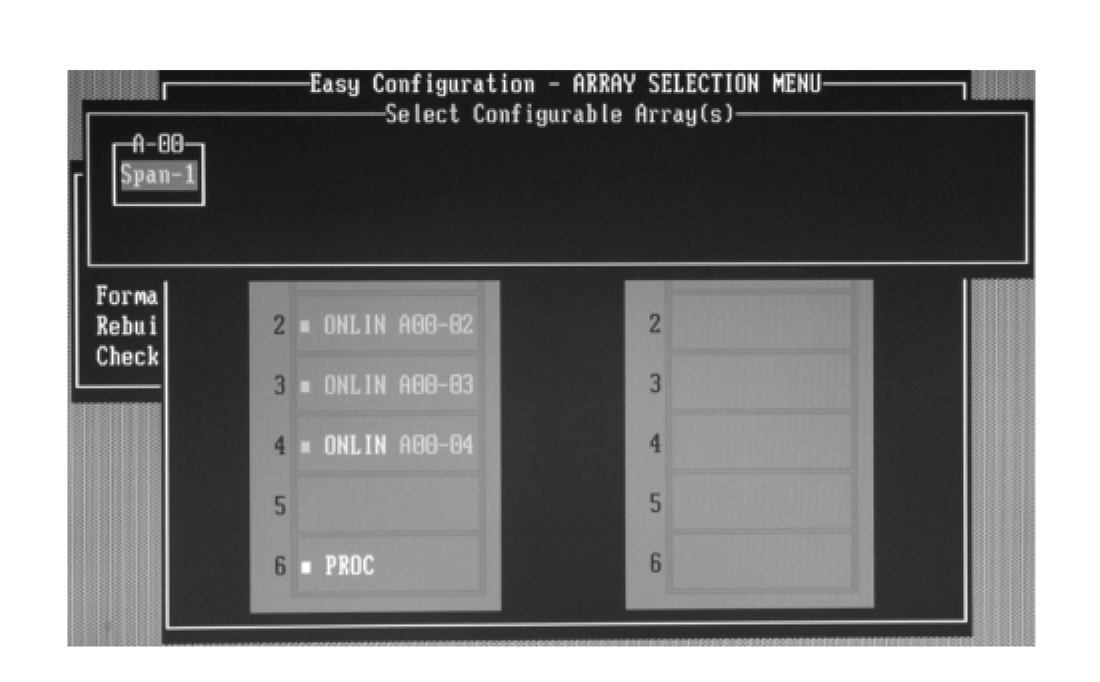


图 2-5 选择 RAID 卡通道

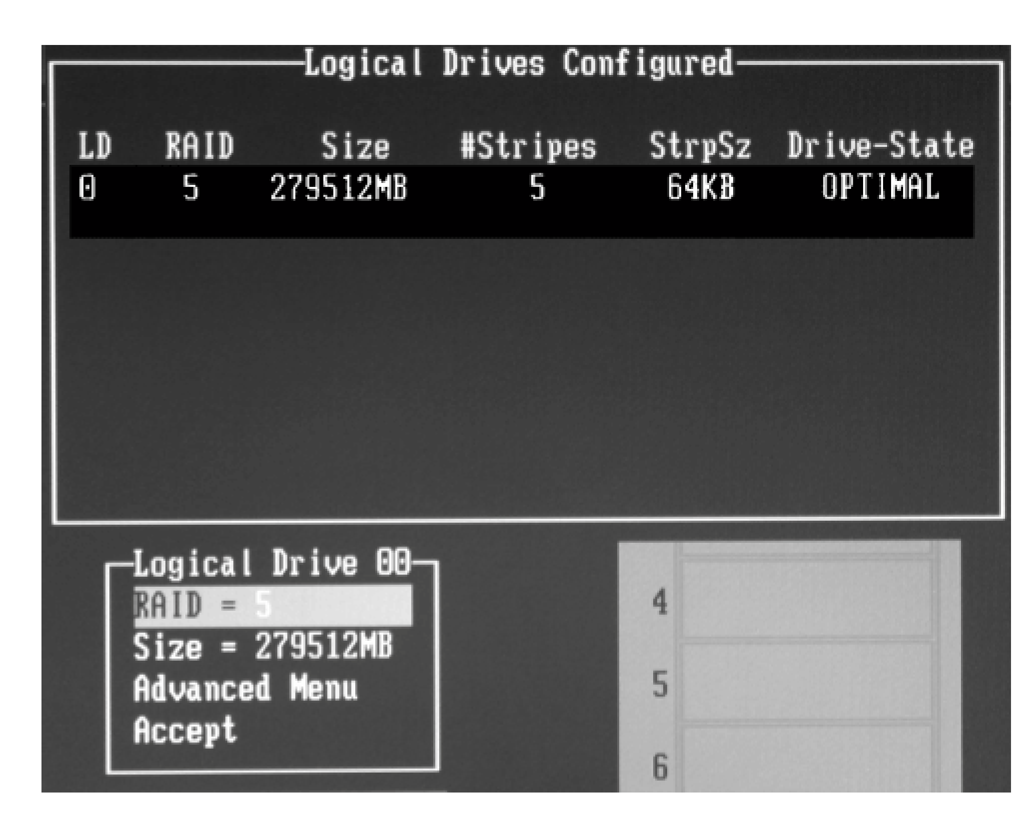


图 2-6 选择 RAID 5 级别

当服务器只安装有两块硬盘时，则默认级别为 RAID 1，如图 2-7 所示。

注意：若要设置为其他级别，可以使用方向键使 RAID=选项反亮显示，然后进行修改。

(7) 移动光标使 Accept 选项反亮显示，并按 Enter 键，系统提示是否保存设置，如图 2-8 所示。移动光标使 YES 选项反亮显示并按 Enter 键，即可完成 RAID 卡的设置。

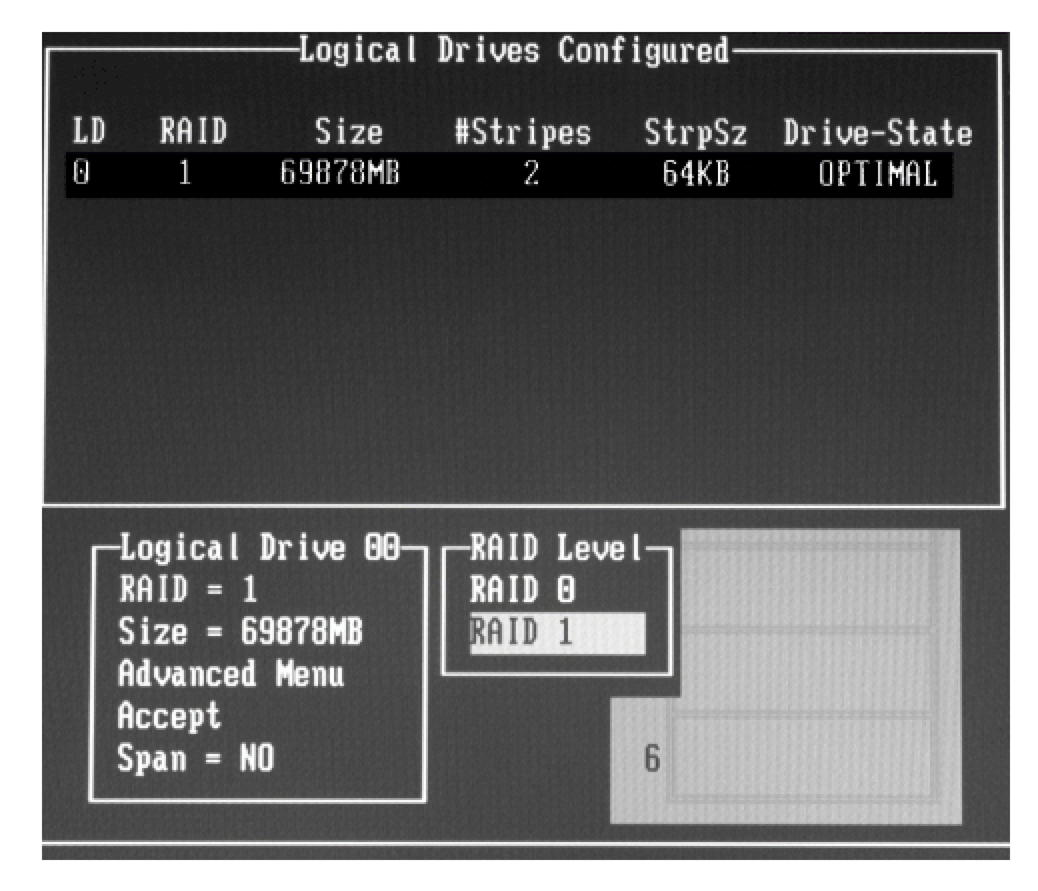


图 2-7 选择 RAID 1 级别

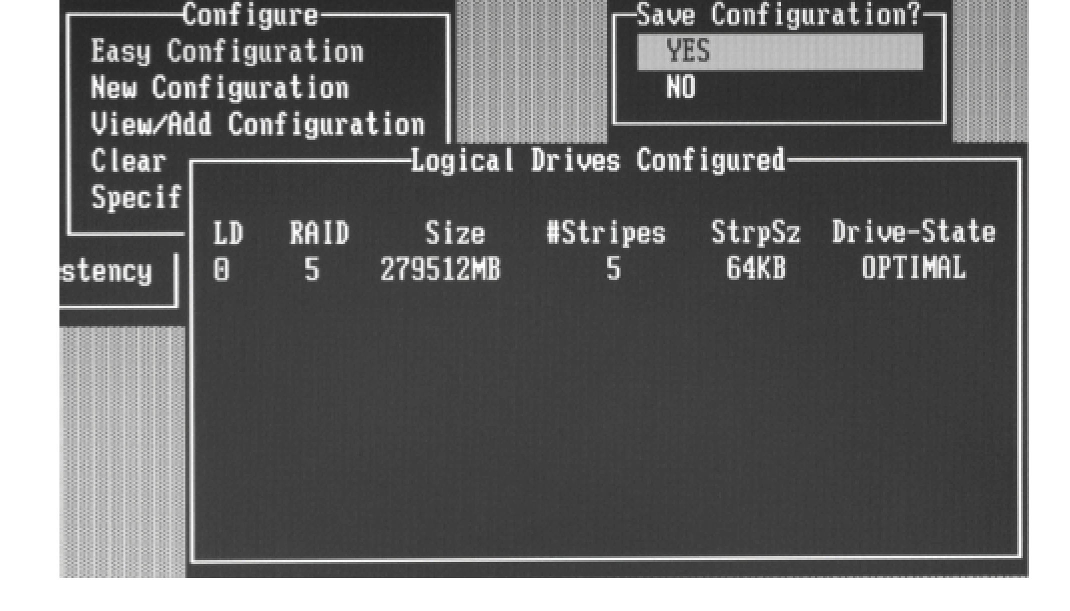


图 2-8 保存 RAID 设置

(8) 根据系统提示，重新引导计算机，即可将全部硬盘视为一块硬盘进行管理。需要注意的是，设置 RAID 的时间可能会比较长，根据硬盘容量的大小不同，所使用时间也有所不同。

注意：RAID 卡的设置应当在操作系统安装之前进行。另外，重新设置 RAID 时，将删除所有硬盘中的全部内容。

2.2.2 Windows Server 2008 RAID 5 的设置

顾名思义，软 RAID 就是不使用 RAID 卡，而是通过系统软件实现 RAID 技术。另外，必须在多磁盘的环境下才可以实现，实现 RAID 1 至少要拥有两块磁盘，实现 RAID 5 至少要拥有 3 块磁盘，这里以 RAID 5 为例进行介绍。

(1) 依次选择“开始”→“管理工具”→“计算机管理”命令，打开“计算机管理”窗口，依次展开“系统工具”→“存储”→“磁盘管理”选项，显示图 2-9 所示的“磁盘管理”窗口。

(2) 右击“磁盘 1”并选择快捷菜单中的“新建 RAID-5 卷”命令，显示“欢迎使用新建 RAID-5 卷向导”对话框。

(3) 单击“下一步”按钮，显示图 2-10 所示的“选择磁盘”对话框，在这里可以选择磁盘并为此卷设置磁盘大小。在“可用”磁盘列表中选中要使用的磁盘，单击“添加”按钮将其添加到“已选的”磁盘列表中。

(4) 单击“下一步”按钮，显示图 2-11 所示的“分配驱动器号和路径”对话框，选中“分配以下驱动器号”单选按钮，为该 RAID 5 卷指派驱动器号。

(5) 单击“下一步”按钮，显示图 2-12 所示的“卷区格式化”对话框。要在卷区上存储数据，必须先将其格式化。选中“按下列设置格式化这个卷”单选按钮，并采用默认的 NTFS 文件系统和分配单位大小。为了便于区分和管理，还可以在“卷标”文本框中为该 RAID 5 卷指定一个卷标名，也可以保持为空。



图 2-9 “磁盘管理”窗口



图 2-10 “选择磁盘”对话框

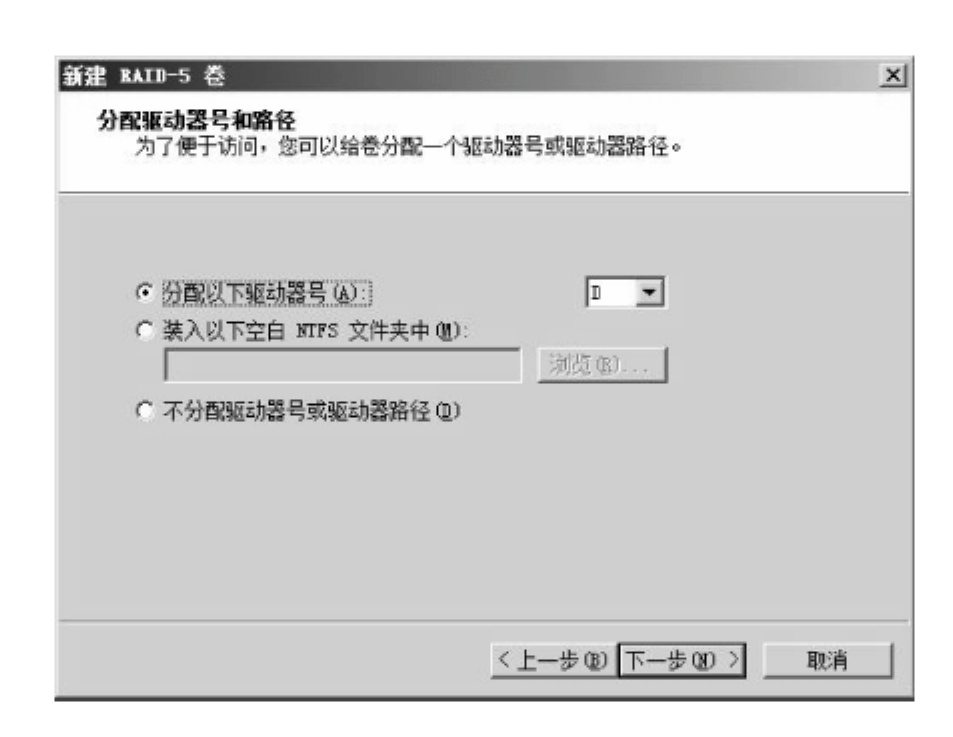


图 2-11 “分配驱动器号和路径”对话框

(6) 单击“下一步”按钮，显示“正在完成新建 RAID-5 卷向导”对话框，在“您已选择下列设置”列表框中核对信息，如不正确单击“上一步”按钮，可重新进行设置。

(7) 单击“完成”按钮，显示图 2-13 所示的“磁盘管理”对话框。提示用户创建 RAID 过程中，所选磁盘将自动转换为动态磁盘，同时该磁盘上原有的操作系统也将丢失。

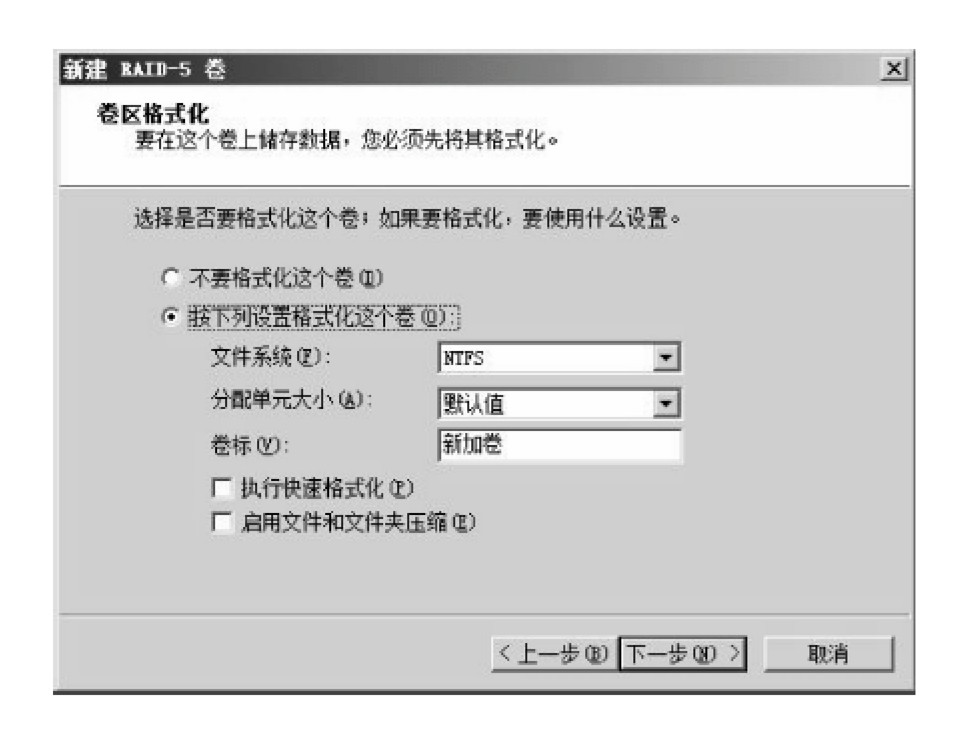


图 2-12 “卷区格式化”对话框



图 2-13 “磁盘管理”对话框

(8) 单击"是"按钮继续创建 RAID 5 卷,完成后返回"磁盘管理"窗口,新创建的 RAID 5 卷即可显示在列表中,如图 2-14 所示。



图 2-14　新建 RAID-5 卷完成

2.2.3　设置磁盘配额

从 Windows 2000 Server 系统开始就提供了卷的磁盘配额功能。在 Windows Server 2008 系统中,管理员同样可以使用该功能控制用户对磁盘空间的占用情况。磁盘配额是以文件所有权为基础的,只应用于卷,且不受卷的文件夹结构及物理磁盘上的布局影响。由于磁盘配额监视个人用户卷的使用情况,因此,每个用户对磁盘空间的利用都不会影响同一卷上其他用户的磁盘配额。

如果要在已经使用的磁盘中启用磁盘配额功能,Windows Server 2008 将计算到启动时间点为止,在该卷中复制文件、保存文件或取得文件所有权的所有用户使用的磁盘空间。根据统计结果,自动为每个用户设置配额限度和警告级别。当然,管理员可以为某个或多个用户设置不同的配额或禁用配额。另外,也可以为还没有在卷上复制文件、保存文件和取得文件所有权的用户设置磁盘配额,或者在一个新创建的卷上启用磁盘配额功能。

使用磁盘配额的过程中,需注意以下内容。

(1) 驱动器的文件格式必须为 NTFS 文件系统格式。如果驱动器的磁盘格式为 FAT32 文件系统,可以使用 Windows Server 2003/2008 提供的文件系统转换工具 Convert 进行转换。

(2) 必须以管理员或管理员组成员的身份登录到 Windows 系统。

1. 启动磁盘限额

在默认的情况下,磁盘配额是没有启用的。启动磁盘配额的操作步骤如下。

(1) 在 Windows 资源管理器中,右击欲启用配额功能的 NTFS 卷,并选择快捷菜单中的"属性"命令,打开"本地磁盘(C:)属性"对话框,选择图 2-15 所示的"配额"选项卡,选中"启用配额管理"复选框,即可启用磁盘配额管理。

选择其中相应的各个选项,以配置系统的磁盘配额功能。

① 选中“拒绝将磁盘空间给超过配额限制的用户”复选框，超过其配额限制的用户，将收到来自 Windows 的“磁盘空间不足”的错误信息，并且在没有从中删除和移动一些现存文件的情况下，无法将额外的数据写入卷中。如果清除该复选框，则用户可以超过其配额限制使用磁盘。

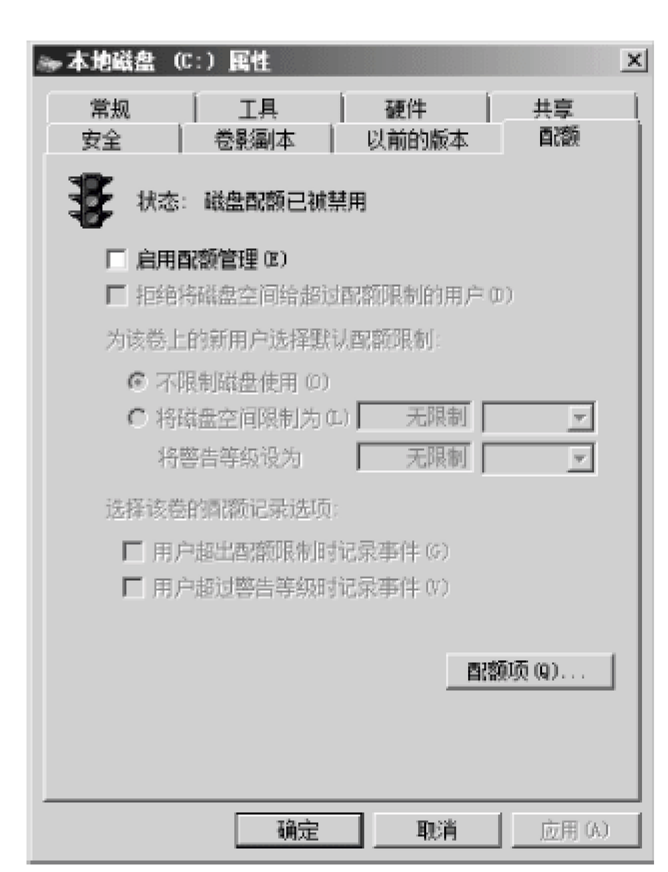


图 2-15 “配额”选项卡

② 选中“将磁盘空间限制为”单选按钮，并输入允许卷的新用户使用的磁盘空间量，以及在将事件写入系统日志前已经使用的磁盘空间量。网络管理员可以在“事件查看器”中查看这些事件。在磁盘空间和警告级别中可以使用十进制数值，从下拉列表框中选择适当的单位（如 KB、MB、GB 等）。

③ 选中“用户超出配额限制时记录事件”复选框，此时如果启用配额，则只要用户超过其配额限制，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

④ 选中“用户超过警告等级时记录事件”复选框，此时如果启用配额，则只要用户超过其警告级别，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

(2) 单击“确定”按钮，保存所做设置，启用磁盘配额完成。

启用磁盘配额管理后，所有的用户都使用磁盘配额启动时设置的默认配额限制和配额警告级别。使用配额项目管理可以为每一个用户设置适合的磁盘配额，对用户的磁盘配额设置进行维护，并且可以记录每一个用户对磁盘空间的使用情况。

2. 为特定的用户磁盘配额

若想让某一个用户使用更多的空间，可以为该用户单独制定更大的磁盘配额。

(1) 在“本地磁盘（C:）属性”对话框中，选择“配额”选项卡，单击“配额项”按钮，显示图 2-16 所示的“（C:）的配额项”窗口。

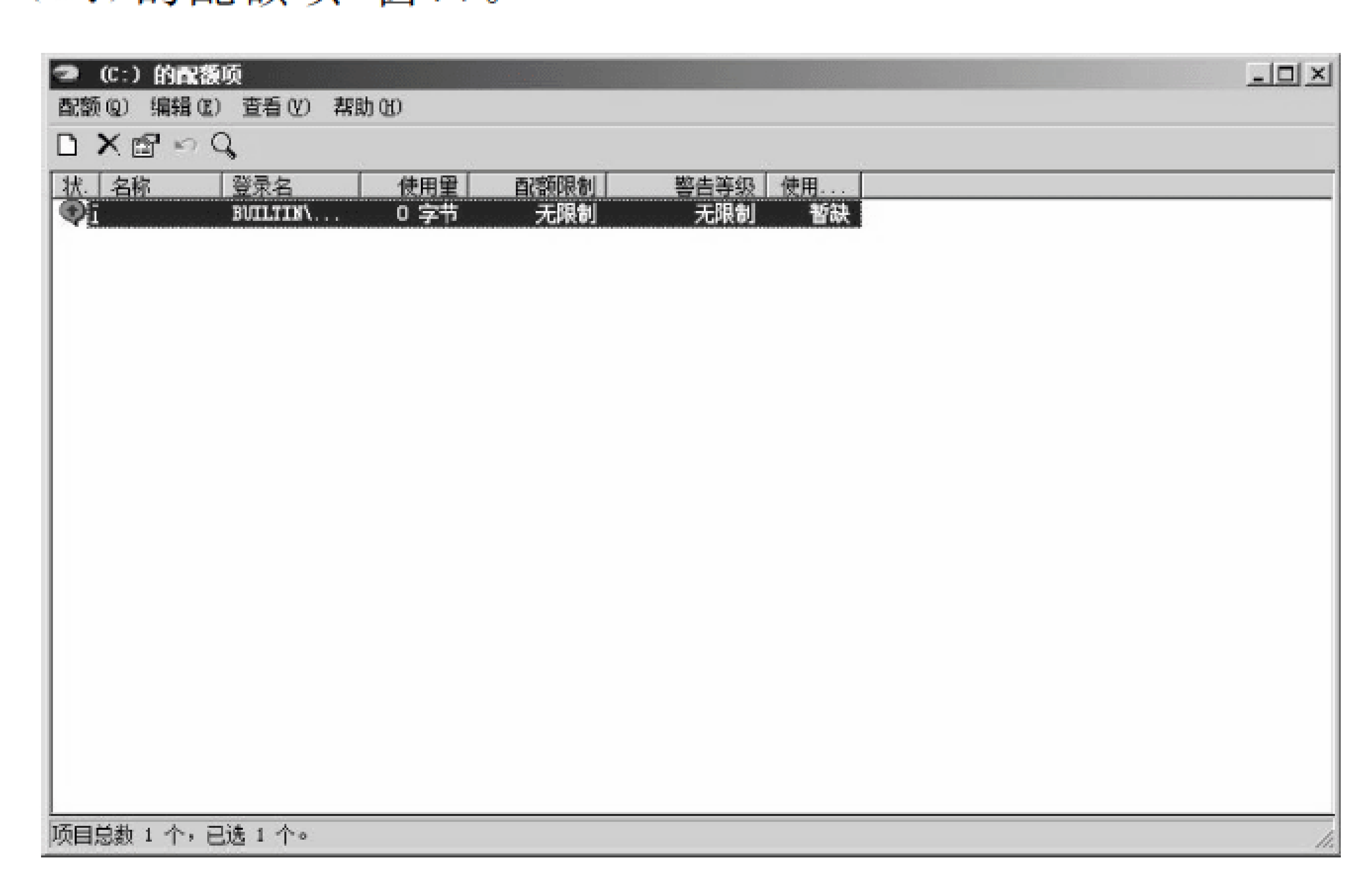


图 2-16 “（C:）的配额项”窗口

(2) 选择“配额”菜单中的“新建配额项”命令,或者单击工具栏中的“新建配额项”按钮,显示图 2-17 所示的“选择用户”对话框。在“选择此对象类型”文本框中显示出当前的对象类型为“用户”,可采用系统的默认值。在“输入对象名称来选择”文本框中,输入要设置配额的用户名称。单击“检查名称”按钮,检查输入的用户账户是否存在。

(3) 单击“确定”按钮,显示图 2-18 所示的“添加新配额项”对话框。选中“将磁盘空间限制为”单选按钮,并在其后文本框中为该用户设置访问磁盘的空间。




图 2-17 “选择用户”对话框

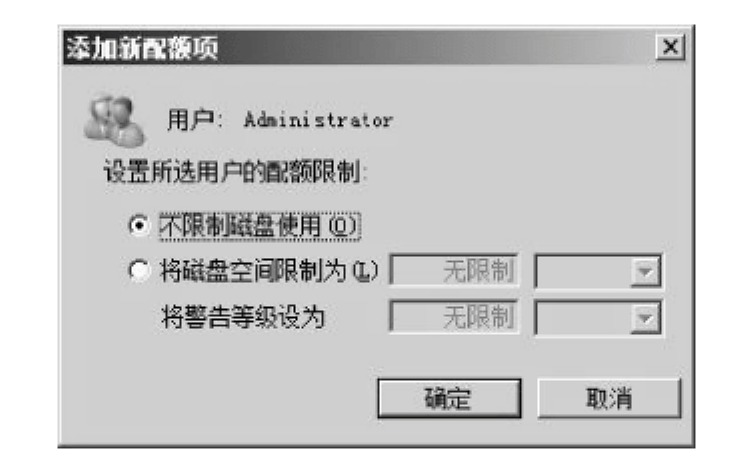


图 2-18 “添加新配额项”对话框

(4) 单击“确定”按钮,保存用户的磁盘配额设置,返回到“(C:)的配额项”窗口,可以看到新创建的用户 Administrator 配额项显示在列表框中,显示如图 2-19 所示。

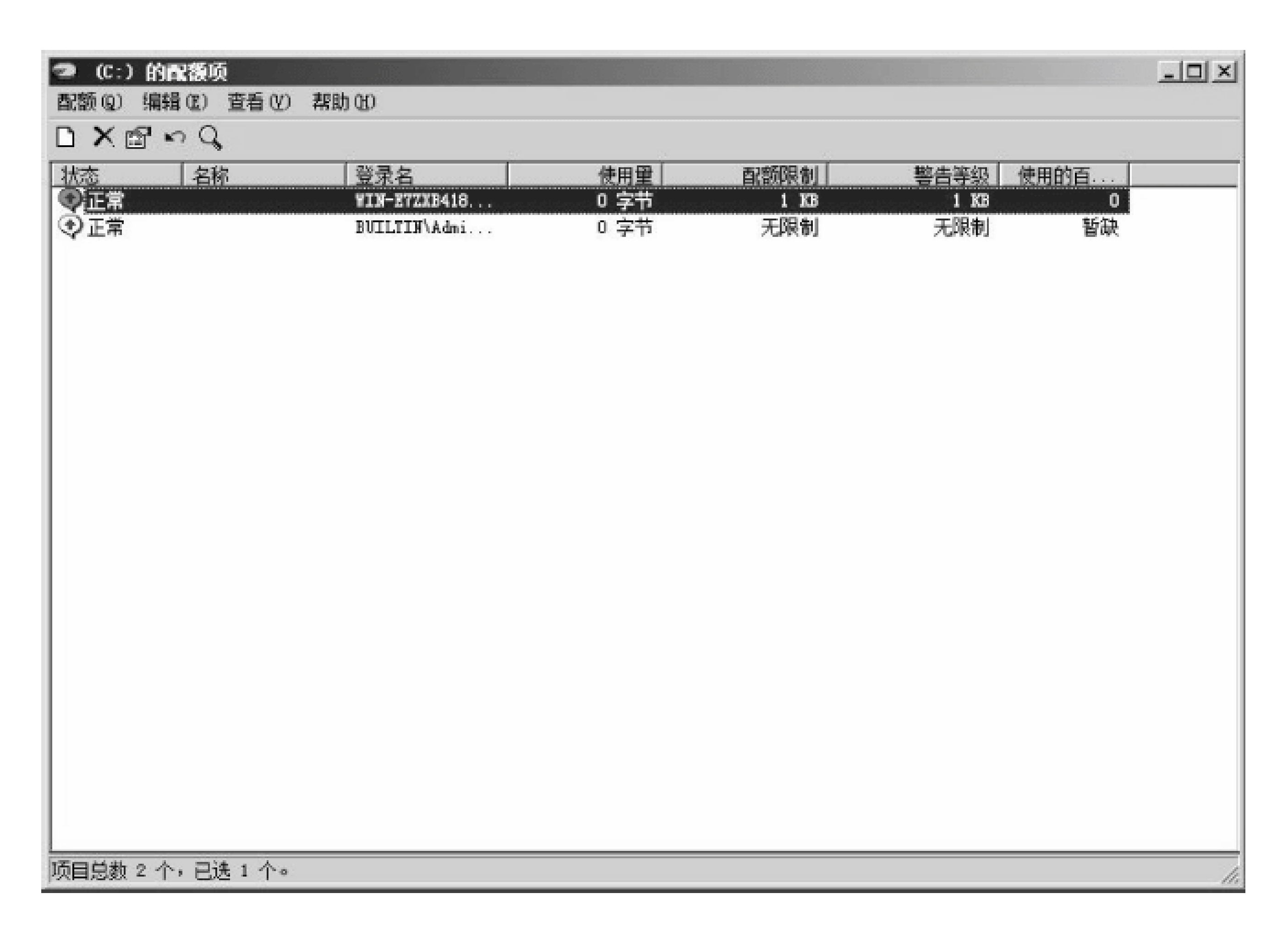


图 2-19 “(C:)的配额项”窗口

如果想删除指定用户的配额项,可选择用户名,右击并选择快捷菜单中的“删除”命令即可。

使用指定配额项具有以下几个优点。

(1) 登录到相同计算机的多个用户之间互不影响。

(2) 一个或多个用户不独占公用服务器上的磁盘空间。

(3) 在个人计算机的共享文件夹中,用户不使用过多的磁盘空间。

3. 监控每个用户的磁盘配额使用情况

当为用户设置好磁盘配额以后,除了可以借助“日志查看器”浏览磁盘占用情况外,在“(C:)的配额项”窗口中,也可以监视每个用户的磁盘配额使用情况,并可单独设置每个用

户可使用的磁盘空间。也就是说配额项的主界面就是一个用户配额监控器。

若欲更改某一个用户的磁盘配额设置，可右击该用户，选择快捷菜单中的“属性”命令，显示图 2-20 所示的配额设置对话框，可以更改用户的磁盘空间限制及警告等级。

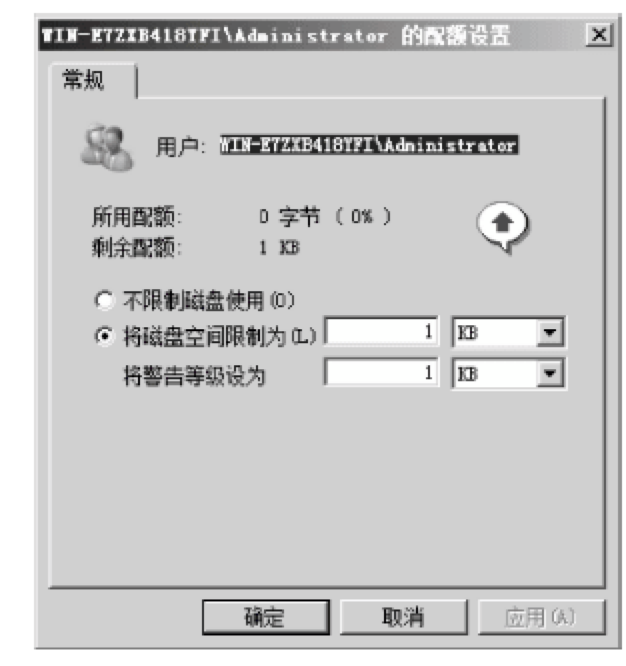


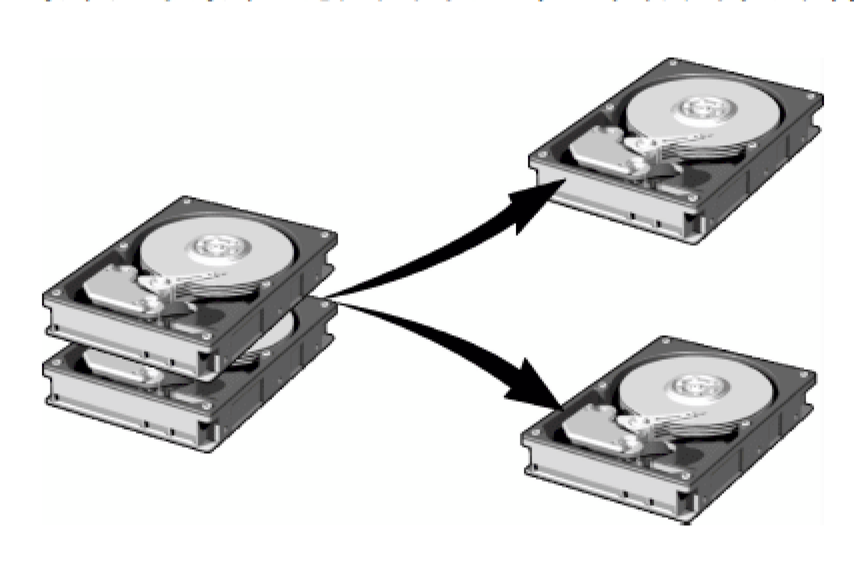
图 2-20　配额设置对话框

2.2.4　知识链接：RAID 介绍

1. RAID 级别及适用范围

RAID(Redundant Array of Independent Disks，独立冗余磁盘阵列)是磁盘阵列实现技术的理论标准，其目的在于减少错误、提高存储系统的性能与可靠度。RAID 原理是利用数组方式作为磁盘组，配合数据分散排列的设计，提升数据的安全性。磁盘阵列主要针对硬盘在容量及速度上无法跟上 CPU 及内存的发展，提出改善方法。

RAID 技术划分为多个级别，分别适用于不同的网络服务和环境。常用的 RAID 级别包括 RAID 0、RAID 1、RAID 0+1 和 RAID 5。需要注意的是，RAID 级别的设置只是为了便于彼此之间的区分，并非高级别就一定比低级别优秀。不同级别的 RAID 各有不同的优点和缺点，适用于充当不同服务的存储设备。


图 2-21　RAID 0 磁盘阵列

(1) RAID 0

RAID 0 又称带区阵列，是一种由两块以上磁盘实现的无冗余磁盘阵列。RAID 0 将数据分割存储到多块硬盘上，磁盘读写时负载平均分配到多块硬盘，由于多块硬盘均可同时读写，所以，速度得以显著提升。图 2-21 所示为由两块磁盘组成的 RAID 0，数据被分别存储在两块磁盘上。

由于数据被分割存储到多块硬盘，所以，数据的完整性依赖于所有硬盘数据均完好无损，任何一块硬盘损坏，都会导致所有数据的丢失。

RAID 0 具有以下优点。

① 存取速度快。由于数据块保存在不同的磁盘上，数据同时在多个硬盘上存取，因此，能成倍地提高磁盘的性能和吞吐量。RAID 的总存取速率几乎是所有磁盘存取速率的总和，所以，数据存取性能非常好。

② 磁盘利用率高。由于所有空间都可以用来保存数据，提供了最大的数据容量，因此，存储空间利用率也是最高的。

③ 存储成本低。由于所有硬盘空间都存储数据，没有任何浪费，所以，单位数据的存储成本最低。

RAID 0 具有以下缺点。

① 不提供冗余数据。RAID 0 系统是最不可靠的，只要有一块硬盘损坏，阵列中所有存储的数据都将全部丢失，而且不可恢复。

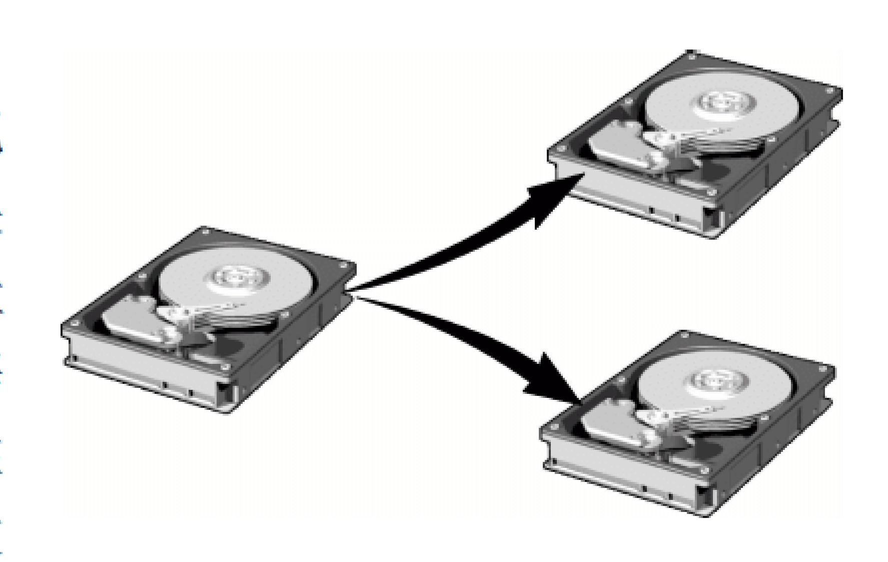
② 不能采用热备份技术。对于一些关键服务任务(如电子商务、数据库)而言，无法实

现双机热备份，无疑是不可接受的。

RAID 0 适用于不需要冗余数据，但对数据存取速度有较高要求，并且必须降低数据存储成本的情况，例如，用于音频和视频点播服务器中多媒体数据的存储。

(2) RAID 1

RAID 1 又称镜像阵列，是一种由两块磁盘实现的冗余磁盘阵列。RAID 1 将同样的数据写入两块硬盘，在两块硬盘上存储完全相同的数据，两块硬盘互为镜像盘，如图 2-22 所示。当一块硬盘中的数据受损或磁盘故障时，另一块硬盘可继续工作，并可在更换硬盘后重新创建镜像。由此可见，RAID 1 的技术重点是最大限度地保证系统的可靠性和可修复性。


图 2-22 RAID 1 磁盘阵列

在 RAID 1 阵列中，任何一块磁盘发生故障，都不会影响到系统的正常运行。当一块磁盘失效时，系统会忽略该磁盘，转而使用剩余的镜像盘读写数据。不过，此时的 RAID 系统是在降级模式下运行。也就是说，虽然保存的数据仍然可以继续使用，但是，RAID 系统将不再可靠。如果剩余的镜像盘也出现问题，那么，整个系统就会崩溃。因此，应当及时地更换损坏的硬盘，避免出现新的问题。

更换新盘后，原有数据将被复制到新盘中，称为同步镜像。同步镜像一般需要很长时间，当磁盘容量较大时更是如此。在同步镜像的进行过程中，尽管外界对数据的访问不会受到影响，但是，由于复制数据需要占用部分带宽，所以，系统的性能还是会有所下降。

RAID 1 具有以下优点。

① 数据存储安全。当一个硬盘损坏时，另一个镜像盘将启用，不存在由于硬盘损坏而造成的数据丢失或系统中断。

② 读取速率较高。由于数据可以从任何一个硬盘中读取，所以，读取性能较高。

RAID 1 具有以下缺点。

① 写入速率较低。RAID 1 不能提升磁盘性能，两块硬盘组成 RAID 1 后，容量等于小硬盘的容量，对任何一个磁盘的数据写入都会被复制到镜像盘中。

② 存储成本高。磁盘镜像肯定会提高系统成本，因为所能使用的空间只是所有磁盘容量总和的一半。RAID 1 是所有 RAID 级别中实现成本最高的一种，尽管如此，许多用户还是选择 RAID 1 来保存那些关键性的重要数据。

当数据的高可靠性和系统的整体性能比硬件成本更重要时，可以采用 RAID 1，例如，数据库服务器、文件服务器，以及其他重要的服务器。

(3) RAID 0+1

RAID 0+1 是由 4 块磁盘实现的冗余磁盘阵列。RAID 0+1 综合了 RAID 0 和 RAID 1 的特点，独立磁盘配置成 RAID 0，两套完整的 RAID 0 互相镜像，如图 2-23 所示。

RAID 0+1 具有以下优点。

RAID 0+1 同时集中了 RAID 0 和 RAID 1 的优点，既具有出色的读写性能，又具有非常高的安全性，可以有效保护系统数据安全。

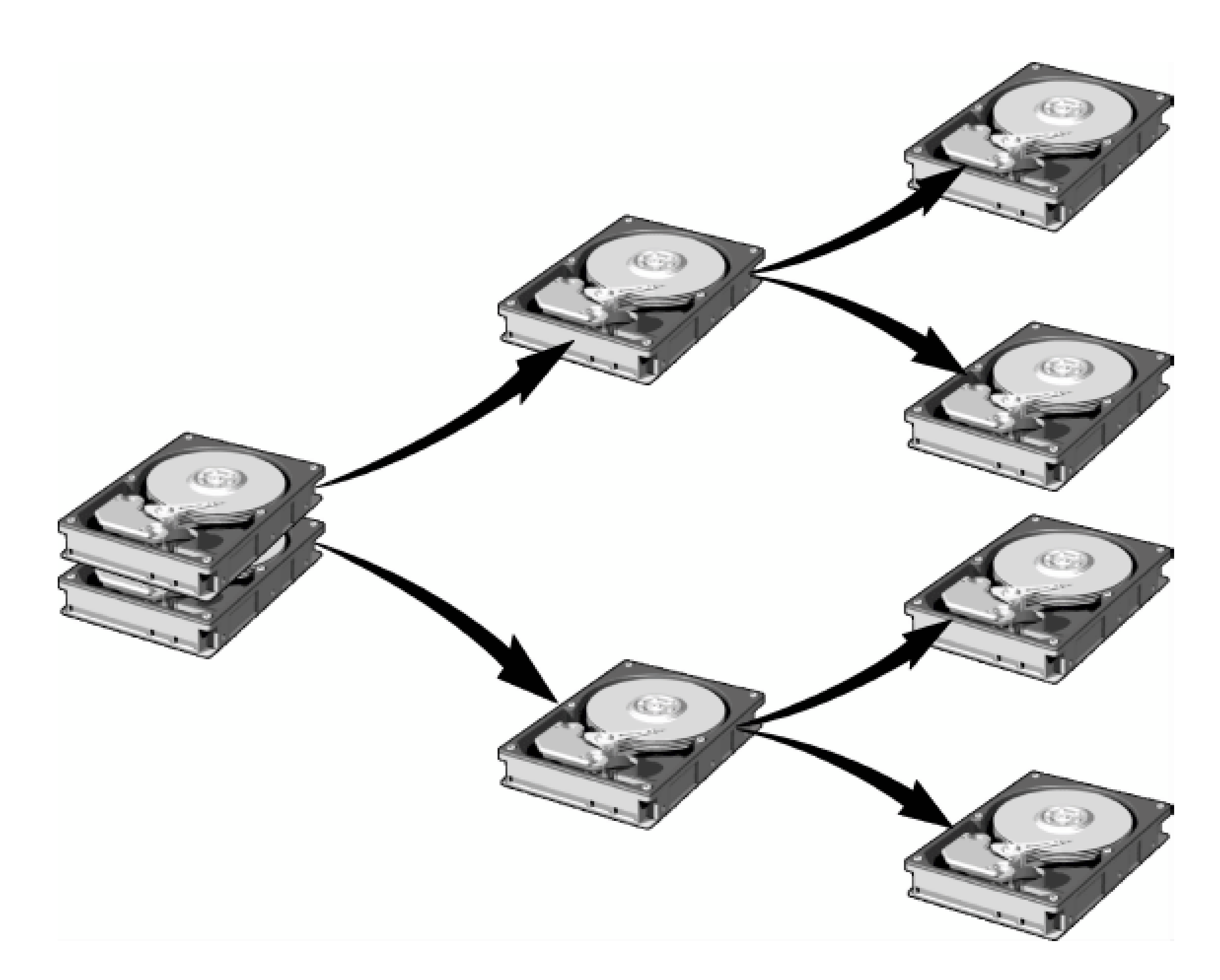


图 2-23 RAID 0+1 磁盘阵列

RAID 0+1 的缺点如下。

构建 RAID 0+1 阵列的成本投入较大，数据空间利用率较低，阵列存储容量只有磁盘总容量的 50%，不能称之为经济高效的方案。

RAID 0+1 适用于既有大量数据需要存取，同时又对数据安全性要求严格的领域，如银行、金融、商业超市、存储库房、各种档案管理等。

(4) RAID 5

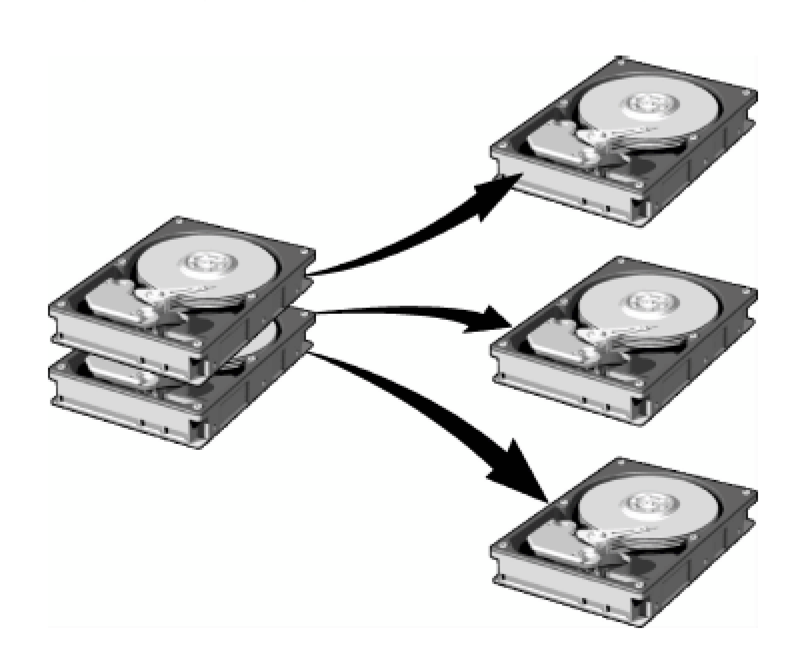


图 2-24 RAID 5 磁盘阵列

RAID 5 是由至少 3 块磁盘实现的冗余磁盘阵列。RAID 5 将数据分布于不同的磁盘上，并在所有磁盘上交叉地存取数据及奇偶校验信息，如图 2-24 所示。如果阵列中的一块磁盘失效，可以按奇偶校验码重建数据，不会导致数据的丢失，并且不影响数据使用。

RAID 5 具有以下优点。

① 数据存储安全。当 RAID 5 阵列中的磁盘损坏时，只需将坏硬盘换掉，RAID 控制系统即可根据校验位，在新盘中重建坏盘上的数据，不会造成数据的丢失。同时，在数据重建过程中，不会影响用户的使用，不会造成数据或系统中断。

② 读取速率较高。RAID 5 不单独指定奇偶盘，读/写指针可同时对阵列设备进行操作，提供了更高的数据流量，更适合于小数据块和随机读写的数据。

③ 磁盘利用率较高。在 RADI 5 阵列中，只有相当于一个磁盘的容量用来存储冗余数据。因此，阵列中的磁盘数量越多，磁盘的利用率就越高。

RAID 5 具有以下缺点。

写入速率较低。RAID 5 有“写损失”，尤其是写许多的小文件和随机数据时更明显。每一次写操作将产生 4 个实际的读/写操作，其中两次读旧的数据及奇偶信息，两次写新的数据及奇偶信息，例如，要改变数据块 1，控制器在计算校验块 1～4 之前，必须先读出数据块 2、数据块 3 和数据块 4，当计算出新的校验块 1～4 后，必须同时写入数据块 1 和校验块 1～4。

在成本、可靠性和性能都同等重要时，可以采用 RAID 5。事实上，RAID 5 被广泛应用

于各种类型的服务器，如文件服务器、应用程序服务器、数据库服务器、Web 服务器、E-mail 服务器等。表 2-1 所示为不同等级 RAID 的特性比较。

表 2-1 不同 RAID 特性

RAID 等级 / 特性	RAID 0	RAID 1	RAID 5
别名	条带	镜像	分布奇偶位条带
容错性	没有	有	有
冗余类型	没有	复制	奇偶位
热备盘选项	没有	有	有
需要的磁盘数	一个或多个	只需两个	三个或更多
可用容量	总的磁盘的容量	只能用磁盘容量的 50%	$(n-1)/n$ 的总磁盘容量。其中 n 为磁盘数

2. RAID 卡简介

硬盘的损坏不仅将直接导致系统瘫痪和网络服务失败，而且还将导致宝贵的存储数据的丢失，所造成的损失往往是难以估量的。为了提高系统的稳定性和数据安全性，服务器通常采用 RAID 卡实现磁盘冗余，既可以确保系统和数据的安全，又可以提高读取速率和存储容量。目前，网络服务器中应用最多的是 SCSI 型 RAID 卡，只是总线有 PCI-X 和 PCI-E 之分。以下为几种不同类型的 SCSI RAID 卡。

(1) SCSI 卡＋Firmware

部分 Ultra320 SCSI 卡提供 RAID 功能，尽管只支持 RAID 0、RAID 1 和 RAID 0＋1，但是性能却不错，并支持 RAID Array 引导。因此，非常适用于中小型网络中的 Web 服务、E-mail 服务和数据库服务。图 2-25 所示为支持 RAID 功能的 LSI Logic 单通道 Ultra320 SCSI 卡 LSI20320-R。

(2) 单通道 SCSI RAID

单通道 SCSI RAID 作为工作组级服务器的基本配置，被应用于存储容量不太大，并且并发访问量也不太大的网络环境。图 2-26 所示为单通道的 Adaptec SCSI RAID 2110S Board。



图 2-25 LSI Logic LSI20320-R

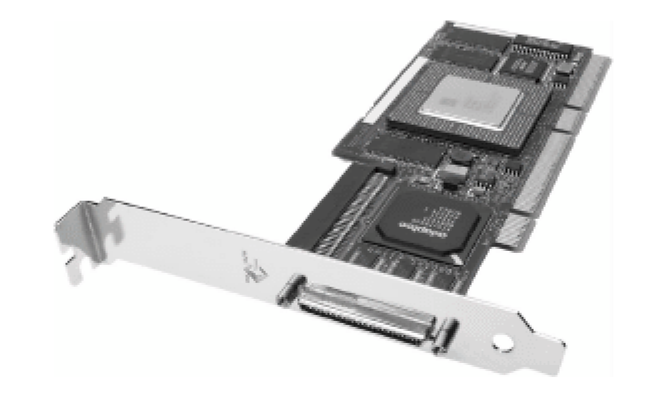


图 2-26 Adaptec SCSI RAID 2110S Board

(3) 双通道 SCSI RAID

双通道 SCSI RAID 作为部门服务器的标准配置，可支持 30 个硬盘。双通道 RAID 拥有更大的 Cache 和更快的处理器，以提高读写速率和性能。图 2-27 所示为双通道的 Adaptec SCSI RAID 2230SLP Board。

(4) 零通道 SCSI RAID

零通道(Zero Channel RAID，ZCR)SCSI RAID 是利用主板自身的 SCSI 芯片，和一个小型 RAID 卡(带处理器)进行组合构成的 SCSI RAID。零通道 RAID 卡充分利用了板载

的 SCSI 芯片，从而以最低的成本，实现了 SCSI 卡到 SCSI RAID 卡的升级。需要注意的是，零通道 RAID 卡必须配合新一代 SO-DIMM 升级槽，或者有特别 BIOS 的主板才可使用。图 2-28 所示为零通道的 Adaptec 2020ZCR Zero Channel RAID。

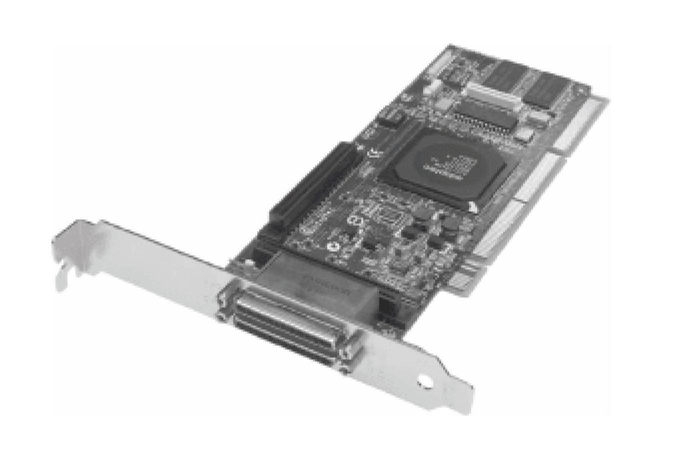




图 2-27 Adaptec SCSI RAID 2230SLP Board

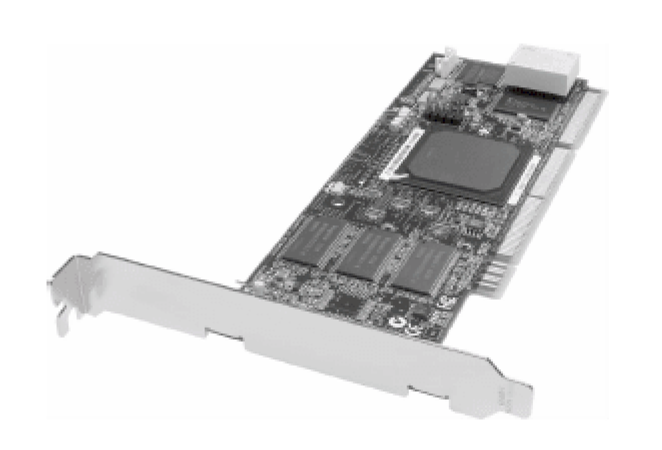


图 2-28 Adaptec 2020ZCR Zero Channel RAID

RAID 卡的主要参数包括支持的 RAID 类型、总线类型、传输速率，以及通道、可连接设备、高速缓存、内部接口和外部接口的数量。另外，通过调整写策略（Write Policy）、读策略（Read Policy）和条带的大小（Stripe Size）等参数，也会影响 RAID 卡的性能。

提示： SCSI RAID 卡应当安装 SCSI 接口硬盘，而 SATA RAID 卡则应当连接 SATA 硬盘。另外，RAID 卡所支持的标准必须与硬盘的标准一致，并且硬盘必须选择同一厂商和同一型号的产品。

2.3 系统服务管理

通常情况下保持系统默认设置即可满足普通用户的日常所需，同时也不会导致严重的系统错误。当有特殊需要必须更改系统服务状态时，也可以谨慎调整。需要注意的是，有些系统服务并不是单独运行的，很可能要依存于其他服务，并且可能有其他正在运行的服务正依存于该服务，操作时应尽量避免“株连”。

2.3.1 系统服务的启用/禁止

系统服务的状态和启动类型是完全不同的两个概念。服务状态是指某系统服务当前的工作状态，只有“已启动”和空白（即关闭）两种状态。启动类型则是前面介绍的跟随系统启动而自动运行或者必要时由用户手动启动，或者直接被禁用等。用户可以通过服务控制台、管理命令或者第三方管理工具来实现对这些系统服务的灵活管理。

1. 服务管理控制台

以 Administrators 组成员身份登录系统，依次选择“开始”→“管理工具”→“服务”命令，打开“服务”管理控制台，如图 2-29 所示。在“服务”窗口可以查看服务名称、描述信息、服务状态、启动方式等。

双击服务可打开该服务的属性窗口，例如双击打开 DHCP Client 服务，或者右击服务名称从快捷菜单中选择“属性”命令，显示图 2-30 所示的“DHCP Client 的属性（本地计算机）”对话框。

在“常规”选项卡的“启动类型”下拉列表框中可以设置该服务的启动方式。如果想停止某个服务，单击“停止”按钮即可；如果服务已经停止，单击“启动”按钮可以开启该服务。根据不同的服务要求，可以在“启动类型”下拉列表框中选择“自动”、“手动”或“禁用”等不同的启动类型。



图 2-29 “服务”管理控制台

(1) 自动：服务随系统启动自动运行，通常用于系统必需服务。

(2) 手动：设置为“手动”类型的系统服务，用户可以根据自己的需要，随时“启动”或“停止”。开启“禁用”类型的服务时，必须先将其设置为“手动”类型。

(3) 禁用：默认关闭的系统服务。

注意：调整完服务的开启状态后，建议重新启动计算机后应用。每一次不要停止太多的服务，这是因为由于不知道哪个服务会发生问题，从而导致系统无法恢复。

如果不确定停止某个服务是否安全，建议采用手动模式。手动模式允许当系统需要某个服务时，由系统管理员去开启该服务，而不是在启动的时候就开启。

若欲指定服务登录时使用的用户账户，选择“登录”选项卡，如图 2-31 所示，可以为服务账户设置不同的登录身份。



图 2-30 服务的启动类型

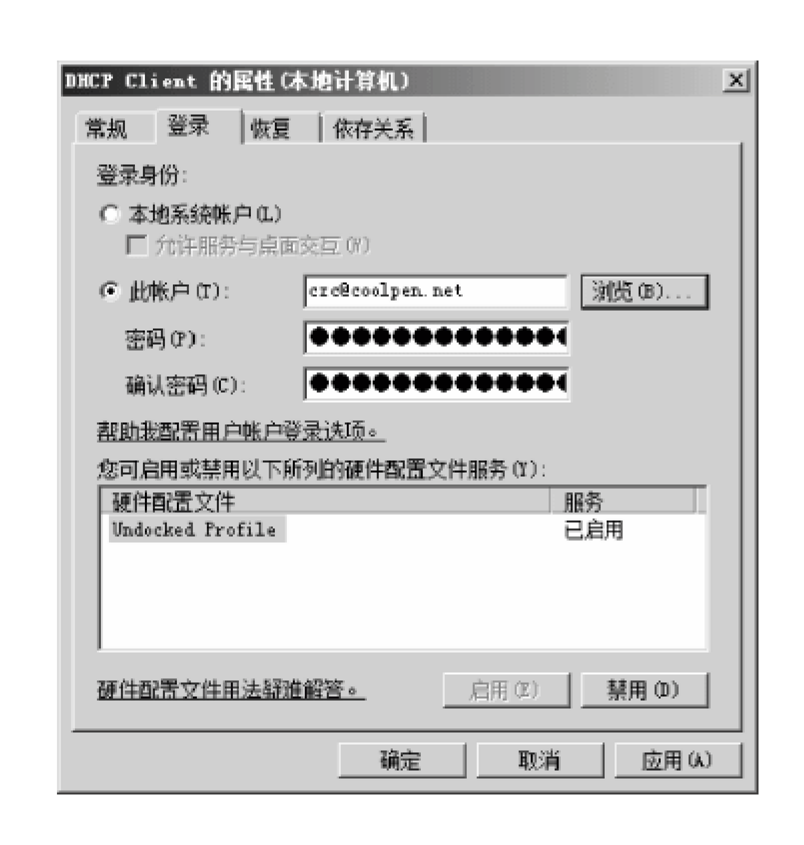


图 2-31 “登录”选项卡

首先，在“登录身份”选项区域中选择适用于此服务的用户账户类型。若要指定服务使用 Local System(本地系统)账户，可以选中“本地系统账户”单选按钮。若要指定服务使用 Network Service(网络服务)账户，可以选中“此账户”单选按钮，然后在账户文本框中输入可以启动此服务的账户，例如 czc@coolpen.net。要指定另一个账户，单击“浏览”按钮，然

后在“选择用户”对话框中指定用户账户。完成操作后，单击“确定”按钮。

在“密码”和“确认密码”文本框中输入网络用户账户的密码，然后单击“确定”按钮。如果选择 Local System 或 Network Service 账户，那么密码必须为空。

注意：更改默认服务设置可能会导致关键的服务无法正常运行，因此，如果服务已配置为“自动启动”，则在更改“启动类型”和“登录为”时一定要非常小心。

在大多数情况下，建议不要更改“允许服务与桌面交互”设置。如果允许服务与桌面交互，则服务在桌面上显示的任何信息也都会显示在交互用户的桌面上。恶意用户可能会获得对该服务的控制权，或从交互桌面攻击它。

如果由于启用或禁用某项服务导致系统启动时发生故障问题，则可以在“安全模式”下启动。这样，只启动必需的核心服务，而加载服务设置的任何更改。计算机进入“安全模式”后，可以更改服务配置或还原默认的配置。

2. 通过硬件配置文件配置相应服务

对于新安装的服务，可能需要设置硬件配置文件来测试，例如，可以为刚安装的服务创建两个硬件配置文件：该服务在一个配置文件中是启用的，而在另一个配置文件中是禁用的。这样，就可以解决任何可能发生的问题(例如驱动程序未正确加载)。

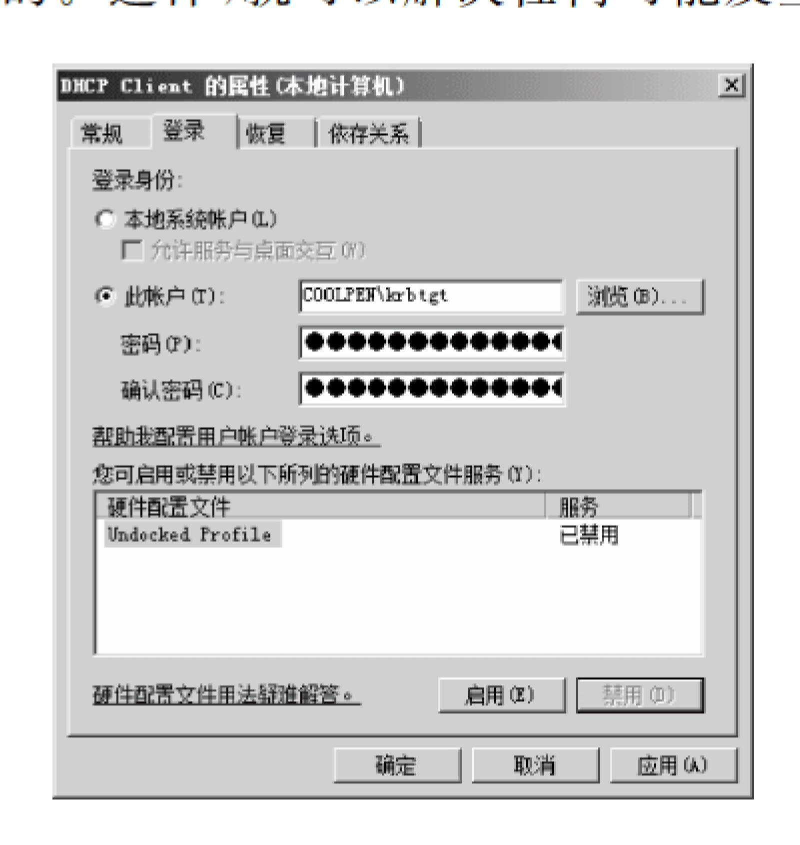


图 2-32 “登录”选项卡

首先打开“服务”控制台，右击服务列表中的服务(仍以 DHCP Client 服务为例)，选择快捷菜单中的“属性”命令，打开“DHCP Client 的属性(本地计算机)”对话框，选择“登录”选项卡，如图 2-32 所示。

其次在“硬件配置文件”列表框中，选择要配置的文件，然后单击“启用”或“禁用”按钮即可。

注意：更改默认服务设置可能导致密钥服务无法正确运行。更改已配置为自动启动的服务的“启动类型”和“登录身份”设置时，谨慎使用。

3. 使用命令开启和停止服务

对于已经被设置为“手动”启动类型，但处于“未启动”状态的系统服务还可以通过专用命令来启动或停止服务。net start 和 net stop 分别用于启动和停止指定系统服务。

(1) net start

net start 命令用于启动一项服务，也可以直接使用不带任何参数的 net start 命令查看当前已经启动的服务，例如直接在命令提示符窗口中输入 net start 并执行，即可显示图 2-33 所示的结果。

net start 命令的基本语法格式为：net start [service]，其中，service 表示启动指定的服务。例如想要启动 messenger 服务，可以在命令提示符窗口中输入 net start server 并执行，成功完成后会显示图 2-34 所示的界面。需要注意的是，服务和应用程序的设置可能根据安装或配置过程中所做的选项设置而变化。

注意：如果服务名包含空格，必须用引号标出，如“routing and remote access”等。

(2) net stop

net stop 命令用于停止正在运行的服务。基本语法格式为：net stop service，其中



图 2-33　显示正在运行的服务

service 表示要停止的服务。例如，要停止正在运行的 DHCP Client 服务，就可以在命令提示符窗口中输入 net stop server 并执行，成功完成后会显示图 2-35 所示的界面。



图 2-34　启动 messenger 服务



图 2-35　停止服务

提示：停止"服务器"服务可以阻止用户访问计算机的共享资源。如果用户使用服务器资源时停止"服务器"服务，则会出现警告消息。y(代表 yes)响应将取消与该计算机的所有连接。

4. 常用的 Windows 服务

Windows 操作系统中，包含了大量的服务，表 2-2 中列出了常用的 Windows 服务，并对对应服务、应用程序关联、在操作系统中是否需要，以及建议的启动类型做了简要的描述，希望用户可以根据服务方面的安全建议，加强计算机系统的安全。

表 2-2　常用的 Windows 服务

服务名称	描　述	应用程序	功能需求	启动类型
Alerter	当系统发生故障时向管理员发送错误警报。通知所选用户和计算机有关系统管理级警报	svchost. exe	不需要	禁用
Application Layer Gateway Service	给予第三者网络共享/防火墙支持的服务，有些防火墙/网络共享软件需要。占用 1. 5MB 内存	alg. exe	可选	手动
Application Management	应用程序管理组件，负责 *. msi 文件格式的安装，但是实际上禁止了该服务并无大碍	svchost. exe	需要	手动

续表

服务名称	描　述	应用程序	功能需求	启动类型
Background Intelligent Transfer Service	在后台传输客户端和服务器之间的数据。如果禁用了 BITS，一些功能(如 Windows Update)就无法正常运行	svchost.exe	不需要	禁用
Base Filtering Engine	基本筛选引擎(BFE)是一种管理防火墙和 Internet 协议安全(IPsec)策略以及实施用户模式筛选的服务。停止或禁用 BFE 服务将大大降低系统的安全。还将造成 IPsec 管理和防火墙应用程序产生不可预知的行为	svchost.exe	需要	自动
ClipBook	用"剪贴簿查看器"储存信息并与远程计算机共享。如果此服务终止，"剪贴簿查看器"将无法与远程计算机共享信息。如果此服务被禁用，任何依赖它的服务将无法启动	clipsrv.exe	不需要	禁用
COM+ Event System	支持系统事件通知服务(SENS)，此服务为订阅组件对象模型(COM)组件事件提供自动分布功能。如果停止此服务，SENS 将关闭，而且不能提供登录和注销通知。如果禁用此服务，显式依赖此服务的其他服务将无法启动	svchost.exe	不需要	手动
COM+System Application	管理基于 COM+组件的配置和跟踪。如果服务停止，大多数基于 COM+组件将不能正常工作。如果本服务被禁用，任何明确依赖它的服务都将不能启动	dllhost.exe	不需要	手动
Computer Browser	维护网络上计算机的更新列表，并将列表提供给计算机指定浏览。如果服务停止，列表不会被更新或维护。如果服务被禁用，任何直接依赖于此服务的服务将无法启动	svchost.exe	可选	自动
Cryptographic Services Windows	提供 3 种管理服务：编录数据库服务，它确定 Windows 文件的签字；受保护的根服务，从此计算机添加和删除受信根证书机构的证书；密钥(Key)服务，它帮助注册此计算机获取证书。如果此服务被终止，这些管理服务将无法正常运行。如果此服务被禁用，任何依赖它的服务将无法启动	svchost.exe	可选	自动
DCOM Server Process Launcher	为 DCOM 服务提供加载功能	svchost.exe	可选	自动
Desktop Window Manager Session Manager	提供桌面窗口管理器启动和维护服务	svchost.exe	可选	自动
DHCP Client	通过注册和更改 IP 地址以及 DNS 名称来管理网络配置	svchost.exe	可选	自动
Distributed Link Tracking Client	用于局域网更新连接信息，比如在计算机 A 有个文件，在计算机 B 做了连接，如果文件移动了，这个服务将会更新信息。占用 4MB 内存	svchost.exe	不需要	手动

续表

服务名称	描述	应用程序	功能需求	启动类型
Distributed Transaction Coordinator	协调跨多个数据库、消息队列、文件系统等资源管理器的事务。如果停止此服务，则不会发生这些事务。如果禁用此服务，显式依赖此服务的其他服务将无法启动	msdtc. exe	不需要	手动
DNS Client	为此计算机解析和缓冲域名系统(DNS)名称。如果此服务被停止，计算机将不能解析 DNS 名称并定位 Active Directory 域控制器。如果此服务被禁用，任何明确依赖它的服务将不能启动	svchost. exe	不需要	自动
Error Reporting Service	服务和应用程序在非标准环境下运行时允许错误报告	svchost. exe	永不	禁用
Event Log	启用在事件查看器查看基于 Windows 的程序和组件颁发的事件日志消息。无法终止此服务	services. exe	需要	自动
Fast User Switching Compatibility	多用户快速切换服务	svchost. exe	不需要	手动
Fax Service	传真服务。需要单独安装	fxssvc. exe	没有安装	没有安装
FTP Publishing Service	发布 FTP 服务，需要单独安装	inetinfo. exe	没有安装	没有安装
Help and Support	启用在此计算机上运行帮助和支持中心。如果停止服务，帮助和支持中心将不可用。如果禁用服务，任何直接依赖于此服务的服务将无法启动	svchost. exe	不需要	没有安装
IIS Admin	本机 IIS 服务管理服务。需要单独安装	inetinfo. exe	没有安装	没有安装
Indexing Service	为本地硬盘或共享网络驱动器的文档内容和属性建立索引的索引服务，超级占用系统资源，建议禁止	cisvc. exe	永不	禁用
Internet Connection Firewall/Internet Connection Sharing	Windows XP 系统的防火墙，为多台计算机联网共享一个拨号网络访问 Internet 提供服务	svchost. exe	可选	自动
IPSEC Services	管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE)和 IP 安全驱动程序	lsass. exe	不需要	禁用
Logical Disk Manager	监测和监视新硬盘驱动器并向逻辑磁盘管理器管理服务发送卷的信息以便配置。如果此服务被终止，动态磁盘状态和配置信息会过时。如果此服务被禁用，任何依赖它的服务将无法启动	svchost. exe	可选	手动
Logical Disk Manager Administrative Service	配置硬盘驱动器和卷。此服务只为配置处理运行，然后终止	dmadmin. exe	可选	手动
Message Queuing	消息队列。需要另外安装	mqsvc. exe	没有安装	没有安装
Message Queuing Triggers	消息队列开关。需要另外安装	mqtgsvc. exe	没有安装	没有安装

续表

服务名称	描述	应用程序	功能需求	启动类型
Messenger	传输客户端和服务器之间的 NET SEND 和 Alerter 服务消息。此服务与 Windows Messenger 无关。如果服务停止，Alerter 消息不会被传输。如果服务被禁用，任何直接依赖于此服务的服务将无法启动	services. exe	不需要	禁用
MS Software Shadow Copy Provider	如果该服务被停止，软件卷影复制将无法管理。如果该服务被停用，任何依赖它的服务将无法启动	dllhost. exe	不需要	手动
Net Login	登录域控制器验证登录信息的服务，支持网络上计算机 pass-through 账户登录身份验证事件	lsass. exe	不需要	禁用
NetMeeting Remote Desktop Sharing	用 NetMeeting 实现远程桌面共享的服务。使授权用户能够通过使用 NetMeeting 跨企业 Intranet 远程访问此计算机。如果此服务被停用，远程桌面服务将不可用。如果此服务被禁用，任何依赖它的服务将无法启动	mnmsrvc. exe	永不	禁用
Network Connections	网络连接服务，管理网络和拨号网络，上网和局域网都需要这个服务，管理“网络和拨号连接”文件夹中的对象，在其中可以查看局域网和远程连接	svchost. exe	必须	手动
Network DDE	为在同一台计算机或不同计算机上运行的程序提供动态数据交换(DDE)的网络传输和安全。如果此服务被终止，DDE 传输和安全将不可用。如果此服务被禁用，任何依赖它的服务将无法启动	netdde. exe	不需要	禁用
Network DDE DSDM	管理动态数据交换(DDE)网络共享。如果此服务终止，DDE 网络共享将不可用。如果此服务被禁用，任何依赖它的服务将无法启动	netdde. exe	不需要	禁用
Network Location Awareness (NLA)	收集并保存网络配置和位置信息，并在信息改动时通知应用程序	svchost. exe	可选	手动
NT LM Security Support Provider	Telnet 服务需要，为使用传输协议而不是命名管道的远程过程调用(RPC)程序提供安全机制	lsass. exe	不需要	禁用
Performance Logs and Alerts	记录机器运行状况而且定时写入日志或发警告，收集本地或远程计算机基于预先配置的日程参数的性能数据，然后将此数据写入日志或触发警报。如果此服务被终止，将不会收集性能信息。如果此服务被禁用，任何依赖它的服务将无法启动	smlogsvc. exe	永不	禁用
Plug and Play	即插即用服务，使计算机在极少或没有用户输入的情况下能识别并适应硬件的更改。终止或禁用此服务会造成系统不稳定	services. exe	必须	自动
Portable Media Serial Number Windows Media	Media Player 和 Microsoft 为保护数字媒体版权认证	svchost. exe	永不	禁用

续表

服务名称	描述	应用程序	功能需求	启动类型
Print Spooler	为打印机提供的服务，在打印的时候开一下即可。可节省 3.8MB 内存	spoolsv.exe	可选	自动
Protected Storage	储存本地密码和网上服务密码的服务，包括填表时的“自动完成”功能。提供对敏感数据(如私钥)的保护性存储，以便防止未授权的服务、过程或用户对其的非法访问	lsass.exe	不需要	自动
QoS RSVP	服务质量资源预留协议。它为 QoS 应用程序预留了 20%的带宽，对于用“猫”上网的用户来说，这 20%的带宽是万万容不得如此铺张浪费的。为依赖质量服务(QoS)的程序和控制应用程序提供网络信号和本地通信控制安装功能	rsvp.exe	不需要	自动
Remote Access Auto Connection Manager	无论什么时候当某个程序引用一个远程 DNS 或 NetBIOS 名或者地址就创建一个到远程网络的连接	svchost.exe	可选	手动
Remote Access Connection Manager	创建网络连接	svchost.exe	可选	手动
Remote Desktop Help Session Manager	远程帮助服务。占用 3.4～4MB 内存。管理并控制远程协助。如果此服务被终止，远程协助将不可用。终止此服务前，参考“属性”对话框上的“依存”选项卡	sessmgr.exe	不需要	禁用
Remote Procedure Call (RPC)	系统核心服务，如果在 Windows Server 2003 中禁止该服务，系统将无法启动。提供终结点映射程序(Endpoint Mapper)以及其他 RPC 服务	svchost.exe	必需	自动
Remote Procedure Call (RPC) Locator	管理 RPC 数据库服务，占用 1MB 内存	locator.exe	不需要	手动
Remote Registry Service	远程注册表运行/修改。使远程用户能修改此计算机上的注册表设置。如果此服务被终止，只有此计算机上的用户才能修改注册表。如果此服务被禁用，任何依赖它的服务将无法启动	svchost.exe	永不	禁用
Removable Storage	可移动存储(如磁带备份等)	svchost.exe	不需要	手动
Routing and Remote Access	在局域网以及广域网环境中为企业提供路由服务	svchost.exe	不需要	禁用
Secondary Logon	给予 Administrator 以外的用户分配指定操作权。启用替换凭据下的启用进程。如果此服务被终止，此类型登录访问将不可用。如果此服务被禁用，任何依赖它的服务将无法启动	svchost.exe	不需要	禁用
Security Accounts Manager	配合 Protected Storage、IIS Admin 的服务	lsass.exe	不需要	自动

续表

服务名称	描　　述	应用程序	功能需求	启动类型
Server	支持此计算机通过网络的文件、打印和命名管道共享。如果服务停止，这些功能不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动	svchost. exe	可选	自动
Simple Mail Transport Protocol (SMTP)	为本机建立跨网传输电子邮件服务，需要单独安装	inetinfo. exe	没有安装	没有安装
Simple TCP/IP Services	需要单独安装，支持一些老的 UNIX 网络服务	tcpsvcs. exe	没有安装	没有安装
SNMP Service	简单网络管理协议，需要单独安装	snmp. exe	没有安装	没有安装
SNMP Trap Service	简单网络管理协议，默认没有安装	snmptrap. exe	没有安装	没有安装
SSDP Discovery Service	UPNP 的硬件利用该服务	svchost. exe	不需要	禁用
System Event Notification	记录用户登录/注销/重启/关机信息。跟踪系统事件，如登录 Windows、网络以及电源事件等。将这些事件通知给 COM＋事件系统“订阅者”(Subscriber)	svchost. exe	不需要	自动
System Restore Service	系统还原服务，占用大量系统资源和内存。执行系统还原功能。要停止服务，从“我的电脑”的属性中的“系统还原”选项卡关闭系统还原	svchost. exe	可选	禁用
Task Scheduler	使用户能在此计算机上配置和制定自动任务的日程。如果此服务被终止，这些任务将无法在日程时间里运行。如果此服务被禁用，任何依赖它的服务将无法启动	svchost. exe	可选	自动
TCP/IP NetBIOS Helper Service	如果网络不用 NetBIOS 或 WINS，就可以关闭。允许对“TCP/IP 上 NetBIOS (NetBT)”服务以及 NetBIOS 名称解析的支持	svchost. exe	不需要	禁用
TCP/IP Printer Server	TCP/IP 打印服务，需要单独安装	tcpsvcs. exe	没有安装	没有安装
Telephony	拨号服务。提供 TAPI 的支持，以便程序控制本地计算机、服务器以及 LAN 上的电话设备和基于 IP 的语音连接	svchost. exe	可选	手动
Telnet	允许远程用户登录到此计算机并运行程序，并支持多种 TCP/IP Telnet 客户，包括基于 UNIX 和 Windows 的计算机。如果此服务停止，远程用户就不能访问程序，任何直接依靠它的服务将会启动失败	tlntsvr. exe	永不	禁用
Terminal Services	实现远程登录本地计算机，快速用户切换和远程桌面功能需要该服务支持。允许多个用户连接并控制一台机器，并且在远程计算机上显示桌面和应用程序。这是远程桌面(包括管理员的远程桌面)、快速用户转换、远程协助和终端服务器的基础结构	svchost. exe	不需要	手动
Upload Manager	用来实现服务器和客户端输送文件的服务，简单文件传输不需要此服务	svchost. exe	不需要	禁用

续表

服务名称	描　　述	应用程序	功能需求	启动类型
WebClient	使基于 Windows 的程序能创建、访问和修改基于 Internet 的文件。如果此服务被终止，将会失去这些功能。如果此服务被禁用，任何依赖它的服务将无法启动	svchost. exe	永不	禁用
Windows Audio	管理基于 Windows 的程序的音频设备。如果此服务被终止，音频设备及其音效将不能正常工作。如果此服务被禁用，任何依赖它的服务将无法启动	svchost. exe	必需	自动
Windows Installer	Windows 的 msi 安装服务	msiexec. exe	需要	手动
Windows Management Instrumentation	提供共同的界面和对象模式以便访问有关操作系统、设备、应用程序和服务的管理信息。如果此服务被终止，多数基于 Windows 的软件将无法正常运行。如果此服务被禁用，任何依赖它的服务将无法启动	svchost. exe	必需	自动
Windows Management Instrumentation Driver Extension	Windows 管理服务扩展	svchost. exe	需要	手动
Wireless Zero Configuration	无线网络设置服务	svchost. exe	可选	禁用
Workstation	用来管理网络、支持联网和打印、文件共享。创建和维护到远程服务的客户端网络连接。如果服务停止，这些连接将不可用。如果服务被禁用，任何直接依赖于此服务的服务将无法启动	svchost. exe	必需	自动
World Wide Web Publishing Service	WWW 服务，需要单独安装	inetinfo. exe	不需要	没有安装

2.3.2　系统服务的设置

服务在启动或者运行的过程中，可能需要其他的服务已经启动作为先决条件，如果相关的服务没有启动，则当前运行的服务可能不能启动成功。

仍以 DHCP Client 服务为例，在“DHCP Client 的属性(本地计算机)”对话框中，选择“依存关系”选项卡，如图 2-36 所示。在“此服务依赖以下系统组件”列表框中展开相应的服务，即可看到所依存的组件；在“以下系统组件依赖此服务”列表中，列出的是所有依赖于此服务的组件，操作时同样需要注意。

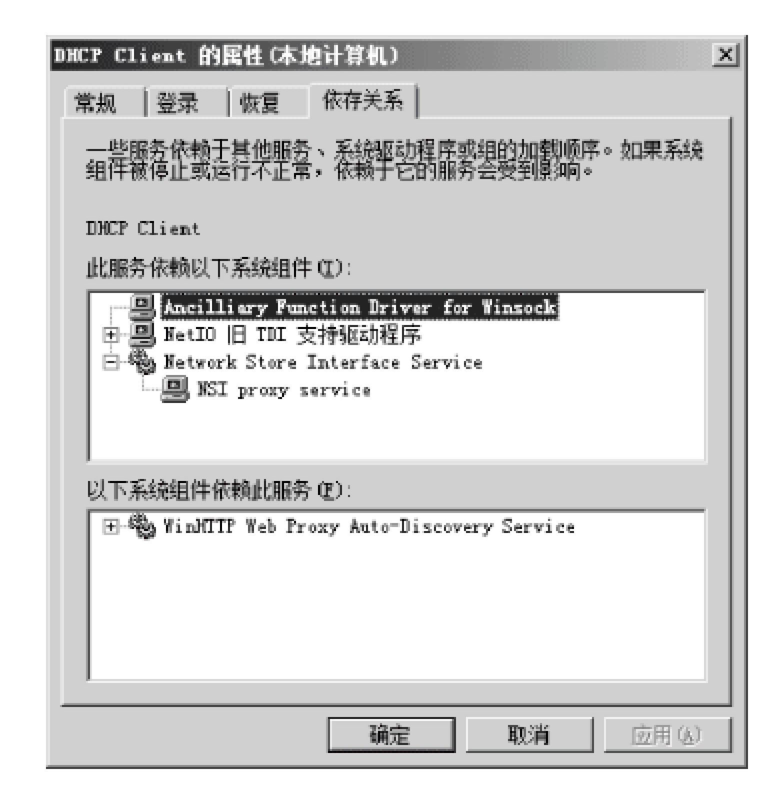


图 2-36　DHCP Client 服务的依存组件

2.3.3　知识链接：PowerShell

PowerShell 是微软公司于 2006 年正式发布的，PowerShell 的发布标志着微软公司向服务器领域迈出了重要的一步。PowerShell 的前身为 Monad，在

2006 年 4 月 25 日正式发布 beta 版时更名为 PowerShell。Windows PowerShell(简称 PS)是一种新的命令行外壳和脚本语言,用于进行系统管理和自动化。Windows PowerShell 建立在.NET Framework 的基础上,可使 IT 专业人员和开发人员控制与自动完成 Windows 及应用程序的管理。

1. Windows PowerShell 功能

PowerShell 引入了 cmdlet(读作 command-let)的概念,每个 cmdlet 是内置的,可以分别使用,组合使用更能发挥其作用。在 PowerShell 中,大多数 cmdlet 都非常简单,例如,"get"cmdlet 用于检索数据,"set"cmdlet 用于建立或更改数据,"format"cmdlet 用于设置数据格式,"out"cmdlet 用于将输出定向到指定的目标。

Windows PowerShell 具有如下功能。

(1) 多达 130 个命令行可以用来执行常见系统管理任务工具。具体包括管理服务、管理流程、管理事件日志、管理证书、修改注册表,以及使用 Windows Management Instrumentation(WMI)。

(2) 学习和使用都非常简单。

(3) 支持用于现有的脚本语言,用于现有的命令行工具,以及多个版本的 Windows,包括 Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 等。

(4) 允许用户浏览数据存储区文件系统。这些数据存储区包括注册表和证书存储。

(5) 用于管理 Windows 数据以不同的存储区和格式的标准实用程序。包括 Active Directory Service Interfaces(ADSI)、Windows Management Instrumentation(WMI)、COM 对象、ActiveX 数据对象(ADO)、HTML 和 XML。

(6) 复杂的表达式分析和.NET Framework 在命令行中的对象的操作。

(7) 可扩展的接口,使独立软件供应商和企业开发人员能够构建自定义 cmdlet。

2. 选择 PowerShell 版本

在使用 PowerShell 前,首先需要根据实际情况选择所使用的 PowerShell 版本。

(1) 英语版。如果运行的是 Windows 英语版操作系统,或除德语、西班牙语、法语、意大利语、日语、朝鲜语、葡萄牙语、俄语、简体中文或繁体中文外的 Windows 版本,则安装 Windows PowerShell 1.0 英语版。

(2) MUI 语言包。如果运行的是 Windows 多语言界面(MUI)版本(以多种语言显示 Windows 界面),首先安装 Windows PowerShell 1.0 英语版,然后安装 Windows PowerShell 1.0 MUI 语言包。需要注意的是,MUI 语言包中并不包含 Windows PowerShell 程序。

注意:*在安装 Windows PowerShell 1.0 之前,必须先卸载任何其他版本的 Windows PowerShell。在安装 Windows PowerShell 1.0 后,不需要重新启动计算机即可使用。*

3. PowerShell 的安装

PowerShell 并不会随系统安装到计算机中,对于 Windows 2000/XP/2003/Vista 而言,必须到微软网站(http://www.microsoft.com/downloads)下载 PowerShell 安装程序。而 Windows 2008 则可以在安装光盘中找到安装文件,并可使用系统提供的服务器管理器进行安装操作。对于 Windows 2000/XP/2003/Vista 系统,PowerShell 的安装非常简单,下载完成后根据安装向导进行安装即可。这里以 Windows 2008 为例,介绍如何安装 PowerShell。

(1) 打开"服务器管理器"窗口,在左侧栏中选择"功能"选项,在右侧窗口中单击"添

加功能"按钮,显示图 2-37 所示的"选择功能"对话框。在该对话框中,选中 Windows PowerShell 复选框。

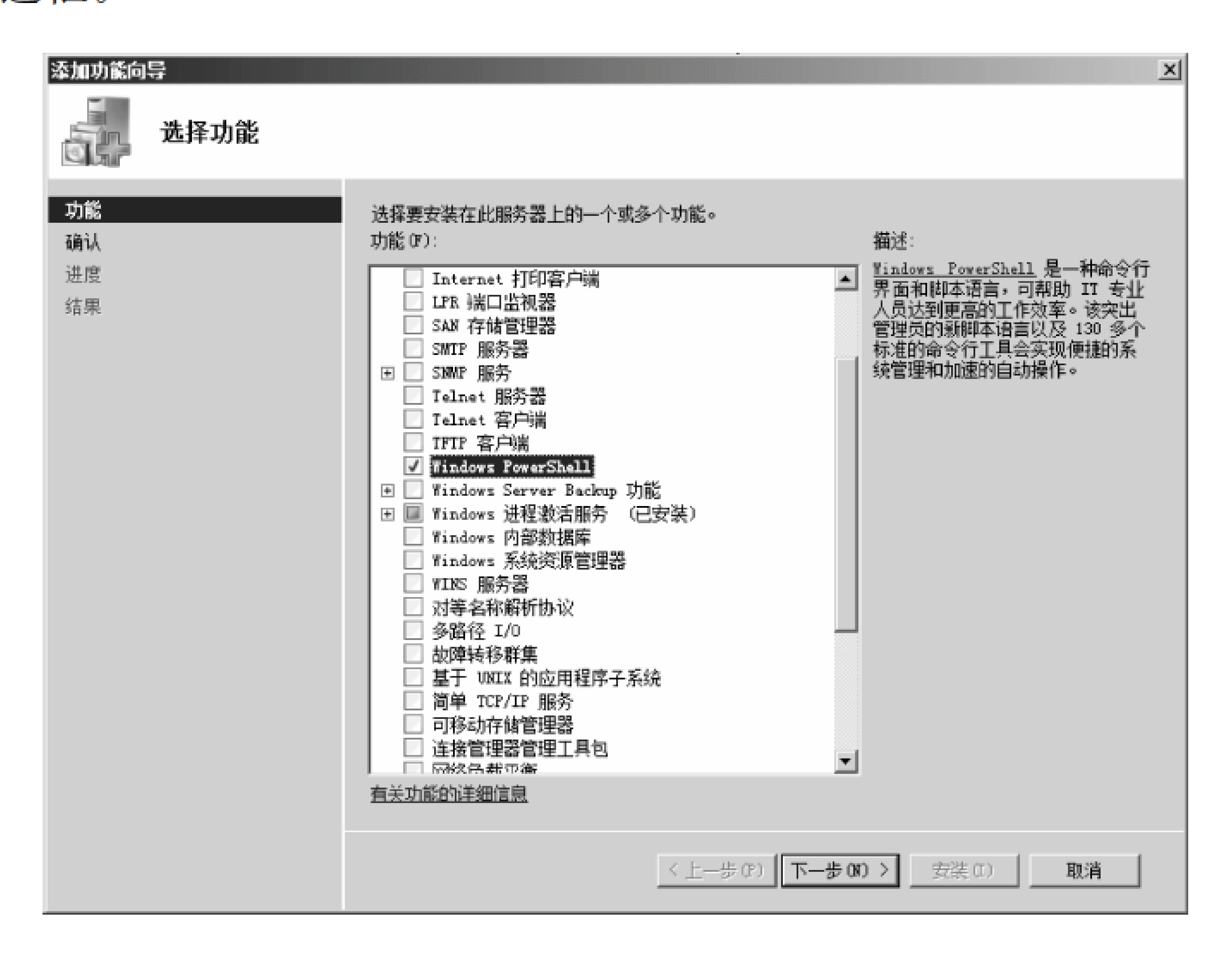


图 2-37　"选择功能"对话框

(2) 单击"下一步"按钮,显示"确认安装选择"对话框。

(3) 确认无误后,单击"安装"按钮,即可开始安装 Windows PowerShell。安装完成后,显示图 2-38 所示的"安装结果"对话框。

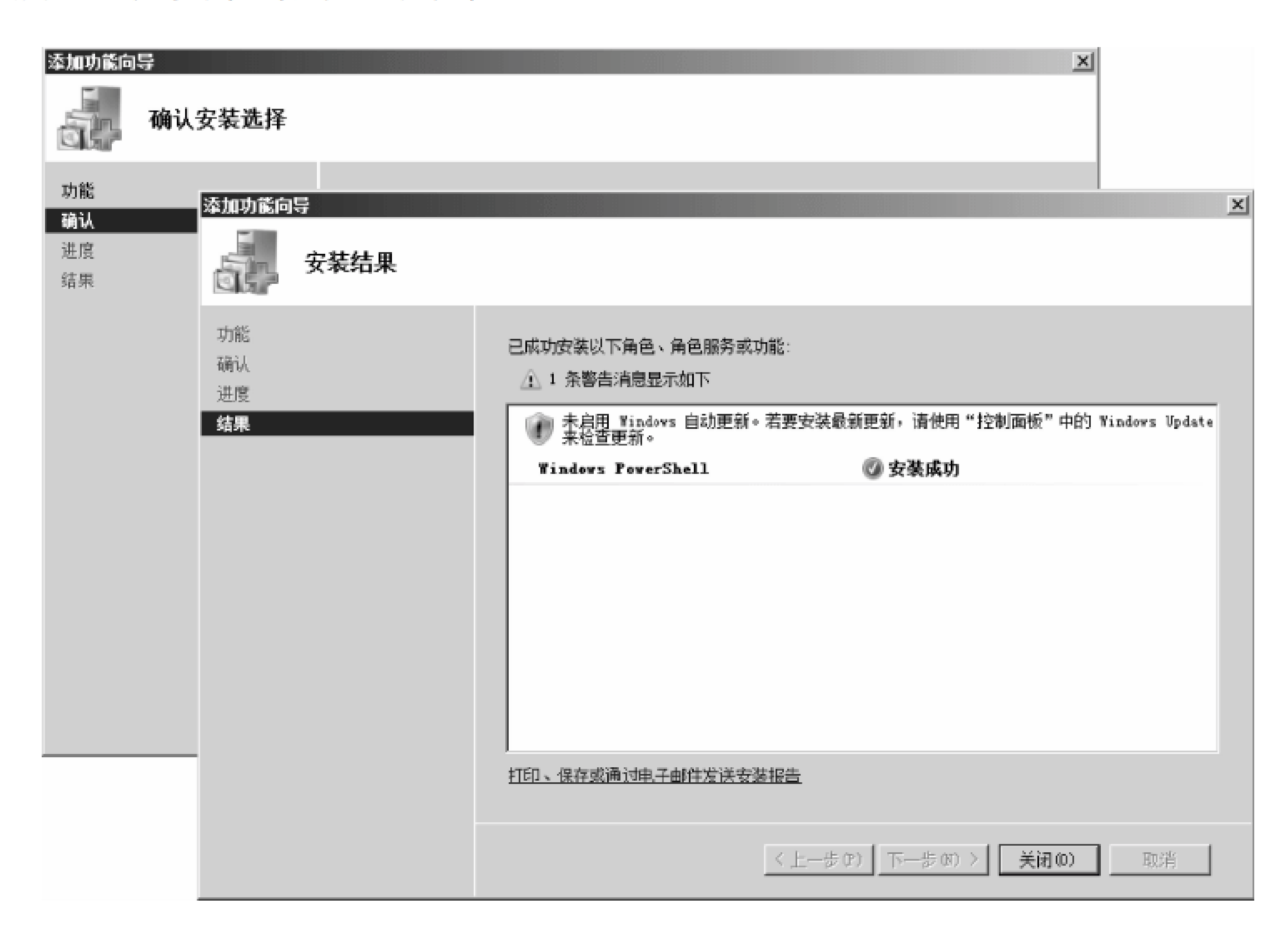


图 2-38　"安装结果"对话框

(4) 单击"关闭"按钮,即可完成该功能的添加操作。

4. 运行 PowerShell

若要运行 PowerShell,可以通过以下 3 种方法实现。

方法 1：依次选择“开始”→“所有程序”→ Windows PowerShell 1.0 → Windows PowerShell 命令，即可启动 PowerShell，如图 2-39 所示。



图 2-39　运行 PowerShell

方法 2：从“运行”对话框中启动 Windows PowerShell。依次选择“开始”→“运行”命令，在“打开”文本框中输入 powershell，然后单击“确定”按钮，即可运行 PowerShell，如图 2-40 所示。

方法 3：在命令提示符下运行 PowerShell，在命令提示符中输入如下命令。

```
powershell
```

按 Enter 键，即可运行 PowerShell，如图 2-41 所示。

图 2-40　从“运行”对话框中启动 Windows PowerShell



图 2-41　在命令提示符下运行 PowerShell

2.4　网络服务管理

使用 MMC 可以简化本地计算机的管理。例如，使用 MMC 管理网络服务，如管理 DHCP 服务器，需要从“管理工具”中运行“DHCP”；如果需要管理 DNS 服务器，就需要运行 DNS；如果需要管理证书服务，就需要运行证书服务。在管理多个服务时，需要频繁地从多种服务中进行切换，而使用 MMC，则可以将常用的管理服务添加到一个 MMC 管理界面中，也可以把本地计算机上的所有管理都添加到一个管理界面中。

(1) 运行 MMC，将本地计算机上的所有欲管理的 MMC 插件添加到一个 MMC 控制台中，如图 2-42 所示。



图 2-42　添加 MMC 控制台

(2) 依次选择“文件”→“保存”命令,显示图 2-43 所示的“保存为”对话框。根据需要设置保存的路径和名称即可,这里将其保存在“管理工具”文件夹下,保存名称为“本地计算机管理”。



图 2-43　“保存为”对话框

(3) 下次使用时,可直接从“管理工具”中运行“本地计算机服务.msc”来管理本地服务。图 2-44 所示为管理域用户。

知识链接:MMC

MMC(Microsoft Management Console)控制台可以根据需要将欲管理的多个管理单元添加到控制台,进行集中管理,例如计算机管理、磁盘管理等。另外,在 MMC 控制台中,还可以将所添加的管理单元进行保存,方便下次使用。图 2-45 所示为添加了磁盘管理、本地用户和组、共享文件夹 3 个管理单元的控制台窗口。具体关于 MMC 控制台的使用方法的介绍可参见第 5 章的相关内容,这里就不再赘述。

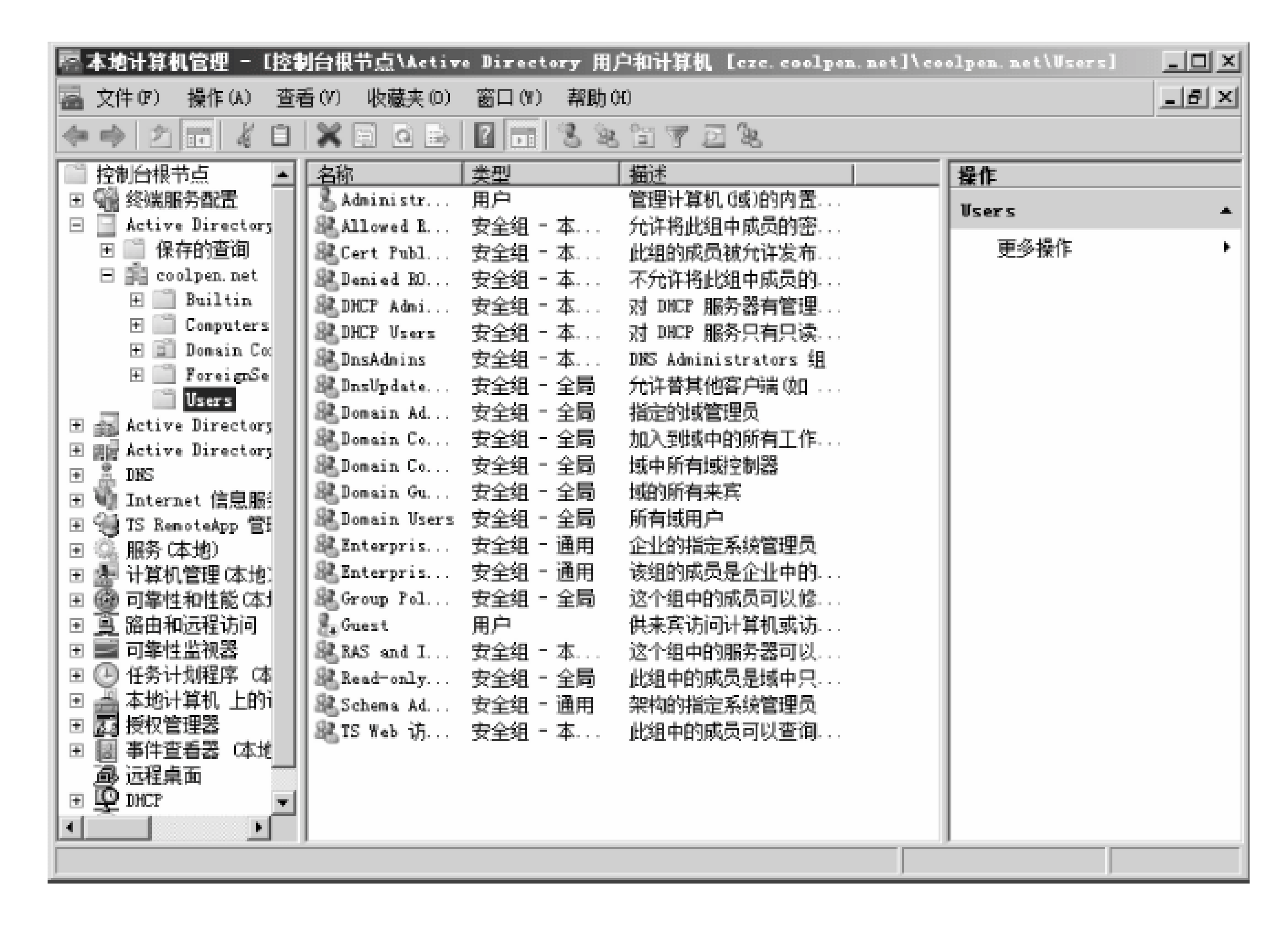


图 2-44　从 MMC 控制台中管理域用户



图 2-45　MMC 控制台

2.5　进程管理

进程是一个具有独立功能的程序关于某个数据集合的一次运行活动，可以申请和拥有系统资源，是一个动态的概念，是一个活动的实体。进程不只是程序的代码，还包括当前的活动，通过程序计数器的值和处理寄存器的内容来表示。

2.5.1　显示任务进程——tasklist

使用 tasklist 命令可以显示运行在本地或远程计算机上的所有任务的应用程序和服务列表，带有进程 ID(PID)。tasklist 是一个进程查看命令，可以查看当前系统中所有运行的进程及占用的内存。

1. 显示任务进程

在命令提示符窗口中输入如下命令。

```
tasklist | more
```

按 Enter 键，即可显示本地计算机中所有正在运行的进程，如图 2-46 所示。在这里显示的进程信息和 Windows 的任务管理器中的是一样的，包含进程名、PID、会话名和占用内存等。

提示：在屏幕显示输出结果后，重复按 Enter 键，可以显示更多任务进程。

```
C:\Users\Administrator>tasklist|more

映像名称                       PID 会话名              会话#
========================= ======== ================ ===========
System Idle Process              0 Services                   0
System                           4 Services                   0
smss.exe                       424 Services                   0
csrss.exe                      492 Services                   0
csrss.exe                      536 Console                    1
wininit.exe                    544 Services                   0
winlogon.exe                   580 Console                    1
services.exe                   620 Services                   0
lsass.exe                      632 Services                   0
lsm.exe                        640 Services                   0
svchost.exe                    784 Services                   0
svchost.exe                    848 Services                   0
svchost.exe                    940 Services                   0
svchost.exe                    988 Services                   0
svchost.exe                   1004 Services                   0
SLsvc.exe                     1020 Services                   0
svchost.exe                   1072 Services                   0
-- More --
```

图 2-46 显示任务进程

2. 显示加载的模块信息

使用 tasklist 命令，显示系统中正在运行的进程信息，同时还显示该进程目前依附的其他模块。在命令提示符窗口中输入如下命令。

```
tasklist /m ¦ more
```

按 Enter 键，显示图 2-47 所示的加载模板的信息。

3. 显示调用指定动态连接库的进程

使用 tasklist 命令，可以看到动态连接库 ntdll. dll 正在使用的那些进程名称。在命令提示符窗口中输入如下命令。

```
tasklist /m ntdll. dll ¦ more
```

按 Enter 键，如图 2-48 所示。

```
C:\Users\Administrator>tasklist /m|more

映像名称                       PID 模块
========================= ======== ============================================
System Idle Process              0 暂缺
System                           4 暂缺
smss.exe                       424 ntdll.dll
csrss.exe                      492 ntdll.dll, CSRSRV.dll, basesrv.dll,
                                   winsrv.dll, USER32.dll, KERNEL32.dll,
                                   GDI32.dll, ADVAPI32.dll, RPCRT4.dll,
                                   LPK.DLL, USP10.dll, msvcrt.dll, sxs.dll
csrss.exe                      536 ntdll.dll, CSRSRV.dll, basesrv.dll,
                                   winsrv.dll, USER32.dll, KERNEL32.dll,
                                   GDI32.dll, ADVAPI32.dll, RPCRT4.dll,
                                   LPK.DLL, USP10.dll, msvcrt.dll, sxs.dll
wininit.exe                    544 ntdll.dll, kernel32.dll, ADVAPI32.dll,
                                   RPCRT4.dll, USER32.dll, GDI32.dll,
                                   msvcrt.dll, USERENV.dll, Secur32.dll,
                                   IMM32.DLL, MSCTF.dll, LPK.DLL, USP10.dll,
                                   apphelp.dll, WS2_32.dll, NSI.dll,
                                   mswsock.dll, wshtcpip.dll, wship6.dll,
                                   credssp.dll, CRYPT32.dll, MSASN1.dll,
                                   schannel.dll, NETAPI32.dll, PSAPI.DLL
winlogon.exe                   580 ntdll.dll, kernel32.dll, ADVAPI32.dll,
                                   RPCRT4.dll, USER32.dll, GDI32.dll,
-- More --
```

图 2-47 加载模板的信息

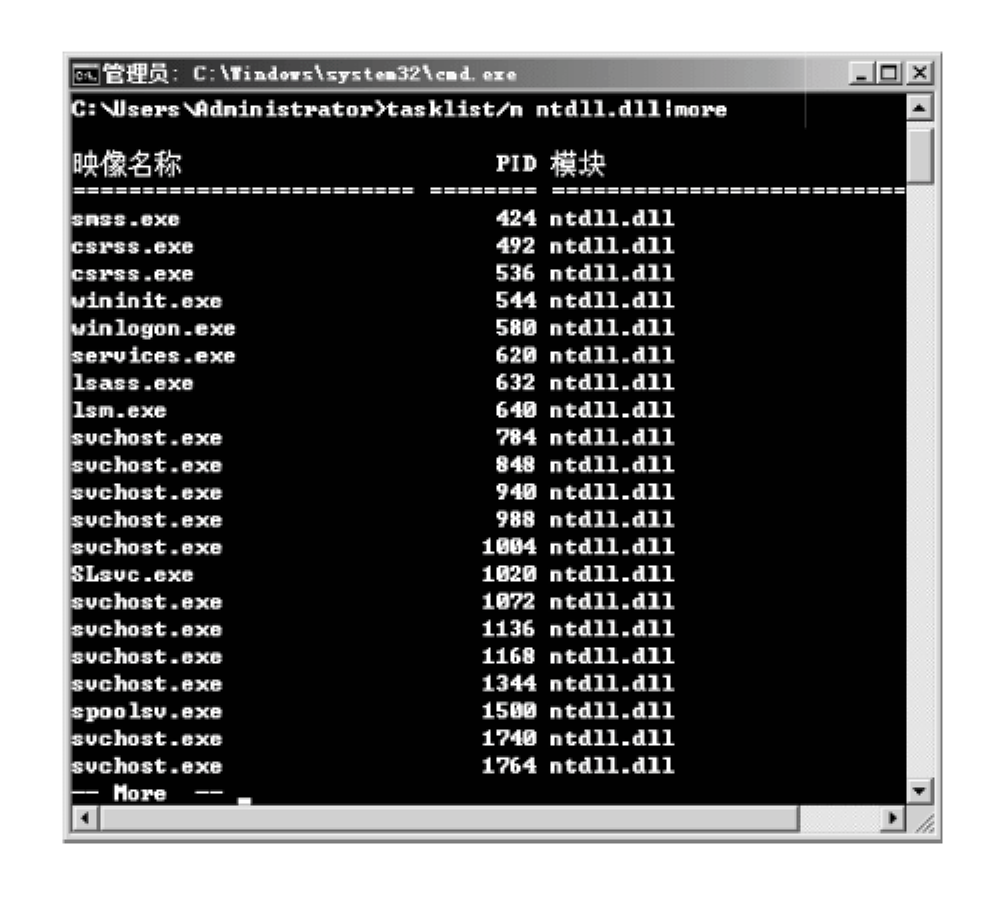


图 2-48 显示调用指定动态连接库的进程

4. tasklist 命令的语法及参数

tasklist 命令的基本语法如下。

```
tasklist [/s system [/u username [/p [password]]]] [/m [module] | /svc | /v] [/fi filter] [/fo format] [/nh]
```

其中，各参数的含义如下。

(1) /s system：指定连接到的远程系统。

(2) /u username：指定执行这个命令的用户。

(3) /p [password]：为提供的用户指定密码。如果忽略，则会提示输入。

(4) /m [module]：列出当前使用所给 exe/dll 名称的所有任务。如果没有指定模块名称，显示所有加载的模块。

(5) /svc：显示每个进程中主持的服务。

(6) /v：显示详述任务信息。

(7) /fi filter：显示一系列符合筛选器指定的标准的任务。

(8) /fo format：指定输出格式。有效值：TABLE、LIST 和 CSV。

(9) /nh：指定列标题不应该在输出中显示。只对“TABLE”和“CSV”格式有效。

表 2-3 列出了有效的筛选器名称、有效操作符和有效值。

表 2-3 有效的筛选器名称、有效操作符和有效值

筛选器名称	有效操作符	有 效 值
STATUS	eq,ne	RUNNING ¦ NOT RESPONDING ¦ UNKNOWN
IMAGENAME	eq,ne	映像名称
PID	eq,ne,gt,lt,ge,le	PID 值
SESSION	eq, ne, gt, lt, ge, le	会话编号
SESSIONNAME	eq, ne	会话名
CPUTIME	eq, ne, gt, lt, ge, le	CPU 时间，格式为 hh:mm:ss。hh: 时，mm: 分，ss: 秒
MEMUSAGE	eq, ne, gt, lt, ge, le	内存使用量，单位为 KB
USERNAME	eq, ne	用户名，格式为 [domain\]user
SERVICES	eq, ne	服务名称
WINDOWTITLE	eq, ne	窗口标题
MODULES	eq, ne	DLL 名称

注意：当查询远程机器时，不支持 WINDOWTITLE 和 STATUS 筛选器。

2.5.2 结束任务进程——taskkill

taskkill 命令用于结束运行在本地或远程计算机上的所有任务的应用程序和服务列表，带有进程 ID(PID)。

例如，结束 explorer.exe 进程，在命令提示符窗口中输入如下命令。

```
taskkill /im explorer.exe
```

按 Enter 键，显示图 2-49 所示的结束资源管理器程序的进程。

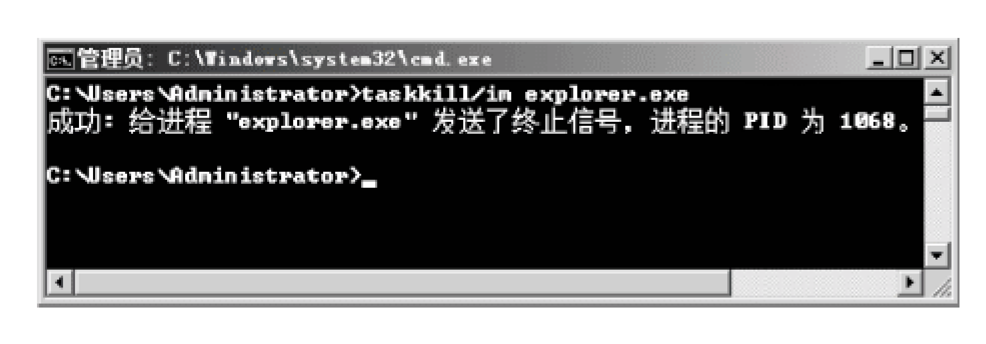


图 2-49 结束 explorer 进程

taskkill 命令的基本语法如下。

```
taskkill[.exe] [/s computer] [/u domain\user [/p password]] [/fo {TABLE|LIST|CSV}] [/nh]
[/fi FilterName [/fi FilterName2 [ ... ]]] [/m [ModuleName] | /svc | /v]
```

该命令中各参数的含义如下。

(1) /s computer：指定远程计算机名称或 IP 地址(不能使用“/”)。默认值是本地计

算机。

（2）/u domain\user：运行具有由 user 或 domain\user. 指定用户的账户权限命令。默认值是当前登录发布命令的计算机的用户权限。

（3）/p password：指定用户账户的密码，该用户账户在/u 参数中指定。

（4）/fo {TABLE|LIST|CSV}：指定输出所用的格式。有效值为 TABLE、LIST 和 CSV。输出的默认格式为 TABLE。

（5）/nh：取消输出结果中的列标题。当/fo 参数设置为 TABLE 或 CSV 时有效。

（6）/fi FilterName：指定该查询包括或不包括的进程类型。表 2-4 列出了相关参数的解释。

表 2-4 参数解释

名 称	运 算 符	值
状态	eq，ne	RUNNING|NOT RESPONDING
Imagename	eq，ne	任何有效字符串
PID	eq，ne，gt，lt，ge，le	任何有效的正整数
会话	eq，ne，gt，lt，ge，le	任何有效的会话数
SessionName	eq，ne	任何有效字符串
CPUTime	eq，ne，gt，lt，ge，le	hh:mm:ss 格式的有效时间。mm 参数和 ss 参数应在 0～59 之间，hh 参数可以是任何一个有效的无符号的数值
memusage	eq，ne，gt，lt，ge，le	任何有效的整数
用户名	eq，ne	任何有效的用户名([domain\]user)
服务	eq，ne	任何有效字符串
Windowtitle	eq，ne	任何有效字符串
Modules	eq，ne	任何有效字符串

（7）/m [ModuleName]：指定显示每个进程的模块信息。指定模块时，将显示使用此模块的所有进程。没有指定模块时，将显示所有模块的所有进程。不能与/svc 或/v 参数一起使用。

（8）/svc：不间断地列出每个进程的所有服务信息。当/fo 参数设置为 TABLE 时有效。不能与/m 或/v 参数一起使用。

（9）/v：指定显示在输出结果中的详细任务信息。不能与/svc 或/m 参数一起使用。

2.5.3 知识链接：命令行

命令行的前身为 DOS，DOS 是 Windows 系列操作系统出现前的一种计算机操作系统。曾经风靡全球，但随着 Windows 操作系统的不断盛行和发展，DOS 已经越来越不受人们关注了。但有些工作依然必须在 DOS 模式下完成，例如系统恢复和修复工作等。因此，在 Windows 2000 以后的版本中，使用命令提示符取而代之。打开“运行”对话框，在“打开”文本框中输入 cmd 命令，单击“确定”按钮，即可启动命令行窗口，如图 2-50 所示。或依次选择“开始”→“所有程序”→“附件”→“命令提示符”命令，也可启动命令行窗口。



图 2-50　命令行窗口

2.6　任务管理

任务计划程序可帮助管理计划在特定时间或在特定事件发生时执行操作的自动任务。该管理单元可以维护所有计划任务的库，从而提供了任务的组织视图以及用于管理这些任务的方便访问点。根据不同的需要可以使用 MMC 控制台或命令行方式，这里以命令行方式为例进行介绍。对于 MMC 控制台方式，可以通过依次选择“开始”→“管理工具”→“任务计划程序”命令，启动“任务计划程序”管理窗口进行配置管理。

使用 schtasks 命令可以对命令和程序进行自定义安排，使其定期运行或在指定时间运行；向计划中添加任务和删除任务、根据需要启动和停止任务以及显示和更改计划的任务；允许管理员创建、删除、查询、更改、运行和中止本地或远程系统上的计划任务。

要显示任务计划，可以在命令提示符下输入以下命令。

```
schtasks
```

按 Enter 键，显示图 2-51 所示的任务计划信息。

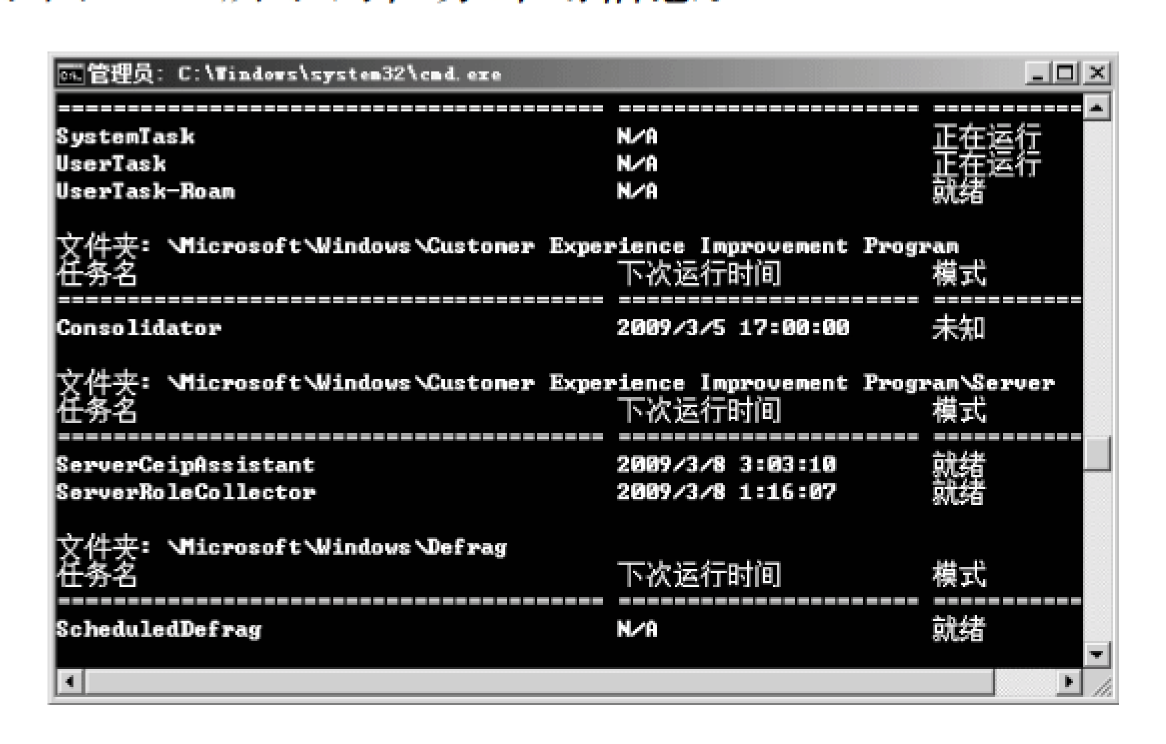


图 2-51　显示任务计划

schtasks 命令的基本语法如下。

```
schtasks /parameter [arguments]
```

其中，/parameter 参数的取值及含义如下。

(1) /create：创建新计划任务。

(2) /delete：删除计划任务。

(3) /query：显示所有计划任务。

(4) /change：更改计划任务属性。

(5) /run：立即运行计划任务。

(6) /end：中止当前正在运行的计划任务。

arguments 参数所使用的选项与/parameter 参数相关，具体选项根据/parameter 参数进行选择。

2.6.1 创建计划任务——schtasks create

schtasks 针对各种计划类型使用不同参数组合。要查看创建任务的组合语法或查看使用特定计划类型创建任务的语法，选择以下选项之一。

(1) 计划任务间隔数分钟运行。

(2) 计划任务间隔数小时运行。

(3) 计划任务间隔数天运行。

(4) 计划任务间隔数周运行。

(5) 计划任务间隔数月运行。

(6) 计划任务在周的指定天运行。

(7) 计划任务在月份的指定周运行。

(8) 计划任务在每月的特定日期运行。

(9) 计划任务在月份的最后一天运行。

(10) 计划任务运行一次。

(11) 计划任务在每次系统启动时运行。

(12) 计划任务在用户登录时运行。

(13) 计划任务在系统空闲时运行。

(14) 计划任务现在运行。

(15) 计划任务以不同权限运行。

(16) 计划任务以系统权限运行。

(17) 计划任务运行多个程序。

(18) 计划任务在远程计算机上运行。

1. 组合语法和参数描述

该命令的基本语法如下。

```
schtasks create /sc ScheduleType /tn TaskName /tr TaskRun [/s Computer [/u [Domain\]User [/p Password]]] [/ru {[Domain\]User | System}] [/rp Password] [/mo Modifier] [/d Day[,Day...]| * ] [/m Month [, Month...]] [/i IdleTime] [/st StartTime] [/ri Interval] [{/et EndTime | /du Duration} [/k]] [/sd StartDate] [/ed EndDate] [/it] [/Z] [/F]
```

该命令中各参数的含义如下。

(1) /sc ScheduleType：指定计划类型。有效值为 MINUTE、HOURLY、DAILY、WEEKLY、MONTHLY、ONCE、ONSTART、ONLOGON、ONIDLE。计划类型 MINUTE、HOURLY、DAILY、WEEKLY、MONTHLY 指定计划的时间单位；ONCE 任务在指定的

日期和时间运行一次；ONSTART 任务在每次系统启动时运行，可以指定启动的日期，或下一次系统启动时运行任务；ONLOGON 每当用户(任意用户)登录时，任务就运行，可以指定日期，或在下次用户登录时运行任务；ONIDLE 只要系统空闲指定的时期，任务就运行，可以指定日期，或在下次系统空闲时运行任务。

(2) /tn TaskName：指定任务的名称。系统上的每项任务都必须具有一个唯一的名称。名称必须符合文件名称规则，并且长度不得超过 238 个字符。使用引号括起包含空格的名称。

(3) /tr TaskRun：指定任务运行的程序或命令。输入可执行文件、脚本文件或批处理文件的完全合格的路径和文件名。路径名称的长度不得超过 262 个字符。如果忽略该路径，schtasks 将假定文件在 Systemroot\System32 目录下。

(4) /s Computer：在指定的远程计算机上计划任务。输入远程计算机的名称或 IP 地址(带有或不带有反斜杠)。默认值是本地计算机。只有使用/s 时，/u 和/p 参数才有效。

(5) /u [Domain\]User：使用指定用户账户的权限运行该命令。默认值为本地计算机上当前用户的权限。只有在远程计算机(/s)上计划任务时，/u 和/p 参数才有效。指定账户的权限用来计划任务和运行任务。要使用其他用户的权限运行任务，需使用/ru 参数。用户账户必须是远程计算机上 Administrators 组的成员。另外，本地计算机必须与远程计算机处于同一个域中，或者必须处于远程计算机域信任的域中。

(6) /p Password：提供在/u 参数中指定的用户账户的密码。如果使用/u 参数，但忽略/p 参数或密码参数，schtasks 将提示输入密码，并且不显示输入的文本。只有在远程计算机(/s)上计划任务时，/u 和/p 参数才有效。

(7) /ru {[Domain\]User | System}：使用指定用户账户的权限运行任务。默认情况下，使用本地计算机当前用户的权限，或者使用/u 参数指定用户的权限(如果包含的话)运行任务。在本地或远程计算机上计划任务时，/ru 参数才有效。值描述[Domain\]User 指定候选用户账户。System 或""指定 Local System 账户，这是一种操作系统和系统服务使用的具有高度特权的账户。

(8) /rp Password：提供在/ru [Domain\]User 参数中指定的用户账户的密码。如果在指定用户账户的时候忽略了这个参数，schtasks. exe 会提示输入密码，而且不显示输入的文本。不要将/rp 参数用于使用系统账户(/ru System)的权限运行的任务。系统账户没有密码，而 schtasks. exe 也不提示输入密码。

(9) /mo Modifier：指定任务在其计划类型内的运行频率。此参数对于 MINUTE、HOURLY、DAILY、WEEKLY 或 MONTHLY 有效，但是可选的，默认值为 1。计划类型修饰符值描述 MINUTE1-1439 任务每 N 分钟运行一次，HOURLY1-23 任务每 N 小时运行一次，DAILY1-365 任务每 N 天运行一次，WEEKLY1-52 任务每 N 周运行一次；ONCE 没有修饰符，任务运行一次，ONSTART 没有修饰符，任务在启动时运行；ONLOGON 没有修饰符，/u 参数指定的用户登录时，运行任务；ONIDLE 没有修饰符，系统闲置/i 参数(需要与 ONIDLE 一起使用)指定的分钟数之后运行任务；MONTHLY1-12 任务每 N 月运行一次；MONTHLYLASTDAY 任务在月份的最后一天运行。MONTHLYFIRST、SECOND、THIRD、FOURTH、LAST 与/dDay 参数一起使用，并在特定的周和天运行任务，例如，在月份的第三个周三。

(10) /d Day[,Day...] | *:指定周或月的一天(或几天)。只对 WEEKLY 或 MONTHLY 计划有效。计划类型修饰符天值(/d)描述 WEEKLY1-52MON-SUN[,MON-SUN...]| * 可选项。MON 是默认值,通配符值(*)指每天,MONTHLYFIRST、SECOND、THIRD、FOURTH、LASTMON-SUN 对于特定周计划是必需的。MONTHLY 无或{1 - 12}1 - 31 仅在没有修饰符(/mo)参数(特定日期计划)的情况下或/mo 为 1 - 12(“每 N 月”计划)时有效并且可选。默认值是 1(月份的第一天)。

(11) /m Month[,Month...]:指定计划任务应在一年的某月或数月运行。有效值为 JAN - DEC。/m 参数仅对 MONTHLY 计划有效。在使用 LASTDAY 修饰符时,这个参数是必需的。

(12) /i IdleTime:指定任务启动之前计算机空闲多少分钟。有效值是从 1～999 的整数。此参数只对 ONIDLE 计划有效,并且是必需的。

(13) /st StartTime:指定任务在一天的什么时间开始(每次开始时间),格式为 HH:MM 24 小时格式。默认值为本地计算机的当前时间。/st 参数只对 MINUTE、HOURLY、DAILY、WEEKLY、MONTHLY 和 ONCE 计划有效。此参数对于 ONCE 计划是必需的。

(14) /ri Interval:指定重复的时间间隔(以分钟计)。此参数不适用于以下计划类型:MINUTE、HOURLY、ONSTART、ONLOGON、ONIDLE。有效范围为 1～599940 分钟(599940 分钟＝9999 小时)。如果指定了/et 或/du,则重复间隔默认为 10 分钟。

(15) /et EndTime:指定“分钟”或“小时”任务计划在一天的什么时间结束,格式为 HH:MM 24 小时格式。指定的结束时间之后,schtasks 不重新启动任务,直到再次达到启动时间。默认情况下,任务计划没有结束时间。该参数是可选的,并且仅对“分钟”或“小时”计划有效。

(16) /du Duration:指定“分钟”或“小时”计划的最大时间长度,格式为 HHHH:MM 24 小时格式。指定的时间过去之后,schtasks 不重新启动任务,直到启动时间再次到来。默认情况下,任务计划没有最大持续时间。该参数是可选的,并且仅对“分钟”或“小时”计划有效。

(17) /k:在/et 或/du 指定的时间停止任务运行的程序。如果没有/k,schtasks 在到达/et 或/du 指定的时间之后不再启动程序,但不会停止仍在运行的程序。该参数是可选的,并且仅对“分钟”或“小时”计划有效。

(18) /sd StartDate:指定任务计划开始的日期。默认值为本地计算机上的当前日期。/sd 参数对于所有计划类型均有效,并且是可选的。StartDate 参数的格式随着“控制面板”的“区域和语言选项”中为本地计算机选择的区域设置而变化。每个区域设置只有一种有效的格式。下面列出了有效的日期格式;使用与本地计算机“控制面板”的“区域和语言选项”中为“短日期”所选格式最为相似的格式,MM/DD/YYYY 用于以月开头的格式,例如英语(美国)和西班牙语(巴拿马);DD/MM/YYYY 用于以日开头的格式,例如保加利亚语和荷兰语(荷兰);YYYY/MM/DD 用于以年开头的格式,例如瑞典语和法语(加拿大)。

(19) /ed EndDate:指定计划结束的日期。此参数是可选的。对于 ONCE、ONSTART、ONLOGON 或 ONIDLE 计划无效。默认情况下,计划没有结束日期。EndDate 参数的格式随着“控制面板”的“区域和语言选项”中为本地计算机选择的区域设置而变化。每个区域设置只有一种有效的格式。下面列出了有效的日期格式:使用与在本地

计算机控制面板的“区域和语言选项”中为“短日期”选择的格式最为相似的格式，MM/DD/YYYY 用于以月开头的格式，例如英语(美国)和西班牙语(巴拿马)；DD/MM/YYYY 用于以日开头的格式，例如保加利亚语和荷兰语(荷兰)；YYYY/MM/DD 用于以年开头的格式，例如瑞典语和法语(加拿大)。

(20) /it：指定只有在“运行方式”用户(运行任务的用户账户)登录到计算机的情况下才运行任务。此参数不影响使用系统权限运行的任务。默认情况下，在计划任务时或使用 /u 参数指定账户(如果使用该参数)时，“运行方式”用户将是本地计算机的当前用户。但是，如果该命令包含 /ru 参数，“运行方式”用户则是由 /ru 参数指定的账户。

(21) /Z：指定在任务计划完成时删除任务。

(22) /F：指定如果指定任务已经存在，就创建任务并取消警告。

2. 计划任务间隔数分钟运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc minute [/mo {1 - 1439}] [/st HH:MM] [/sd StartDate] [/ed EndDate] [{/et HH:MM | /du HHHH:MM} [/k]] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在一个分钟计划中，/sc minute 参数是必需的。/mo(修饰符)参数是可选的，指定了每次运行任务之间间隔的分钟数。/mo 的默认值为 1(每分钟)。/et(结束时间)和/du(持续时间)参数是可选的，并且可与或不与/k(结束任务)参数一起使用。

3. 计划任务间隔数小时运行

(1) 小时计划语法

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc hourly [/mo {1 - 23}] [/st HH:MM] [/sd StartDate] [/ed EndDate] [{/et HH:MM | /du HHHH:MM} [/k]] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在一个小时计划中，/sc hourly 参数是必需的。/mo(修饰符)参数是可选的，指定了每次运行任务之间间隔的小时数。/mo 的默认值为 1(每小时)。/k(结束任务)参数是可选的，并且可与/et(指定时间结束)或/du(指定时间间隔后结束)一起使用。

(2) 每日计划语法

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc daily [/mo {1 - 365}] [/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在每日计划中，/sc daily 参数是必需的。/mo(修饰符)参数是可选的，指定了每次运行任务之间间隔的天数。/mo 的默认值为 1(每天)。

4. 计划任务间隔数周运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc weekly [/mo {1 - 52}] [/d {MON - SUN[,MON - SUN...]| *}] [/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在周计划中，/sc weekly 参数是必需的。/mo(修饰符)参数是可选的，指定了每次运行任务之间间隔的周数。/mo 的默认值为 1(每周)。周计划也拥有一个可选的/d 参数，用于计划任务在一周的指定天或所有天(*)运行。默认值为 MON(星期一)。每天(*)选项相当于计划每日任务。

5. 计划任务间隔数月运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc monthly [/mo {1 - 12}] [/d {1 - 31}] [/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在此计划类型中，/sc monthly 参数是必需的。/mo(修饰符)参数指定每次运行任务之间的月份数，是可选的，默认值为 1(每月)。此计划类型也拥有一个可选的/d 参数，用于计划任务在月份的指定日期运行。默认值是 1(月份的第一天)。

6. 计划任务在周的指定天运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc weekly [/d {MON - SUN[,MON - SUN...]| * }] [/mo {1 - 52}] [/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示："周的天"计划是周计划的变体。在周计划中，/sc weekly 参数是必需的。/mo (修饰符)参数是可选的，指定了每次运行任务之间间隔的周数。/mo 的默认值为 1(每周)。/d 参数是可选的，计划任务在周的指定天或所有天(*)运行。默认值为 MON(星期一)。每天选项(/d *)相当于计划每日任务。

7. 计划任务在月份的指定周运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc monthly /mo {FIRST | SECOND | THIRD | FOURTH | LAST} /d MON - SUN [/m {JAN - DEC[,JAN - DEC...]| * }] [/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在此计划类型中，/sc monthly 参数、/mo(修饰符)参数以及/d(天)参数是必需的。/mo(修饰符)参数指定任务运行的周。/d 参数指定一周中的第几天。(可以仅为此计划类型指定一周中的某一天。)此计划也拥有一个可选的/m(月份)参数，用于针对特定月份计划任务。

8. 计划任务在每月的特定日期运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc monthly /d {1 - 31} [/m {JAN - DEC[,JAN - DEC...]| * }] [/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示：在特定日期计划类型中，/sc monthly 参数和/d(天)参数是必需的。/d 参数指定月份的日期(1～31)，而不是周的天。可以在计划中仅指定一天。/mo(修饰符)参数对此计

划类型无效。/m(月份)参数对此计划类型而言是可选的,默认值为每个月(*)。schtasks不允许针对在/m参数指定的月份中不出现的日期计划任务。但是,如果忽略/m参数,并针对不是在每个月中出现的日期(如31日)计划任务,则该任务不会在较短的月份发生。要针对月份的最后一天计划任务,请使用最后一天计划类型。

9. 计划任务在月份的最后一天运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc monthly /mo LASTDAY /m {JAN - DEC[,JAN - DEC...]}[/st HH:MM] [/sd StartDate] [/ed EndDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示: 在最后一天计划类型中,/sc monthly参数、/mo LASTDAY(修饰符)参数以及/m(月份)参数是必需的。/d(天)参数无效。

10. 计划任务运行一次

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc once /st HH :MM [/sd StartDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示: 在运行一次计划类型中,/sc once参数是必需的。/st参数(指定任务运行时间)是必需的。/sd参数(指定任务运行的日期)是可选的。/mo(修饰符)和/ed(结束日期)参数对此计划类型无效。如果根据本地计算机的时间,指定的日期和时间已经过去,schtasks就不允许计划任务运行一次。要在不同时区的远程计算机上计划任务运行一次,必须在本地计算机上的日期和时间到来之前计划任务。

11. 计划任务在每次系统启动时运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc onstart [/sd StartDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示: 在启动时计划类型中,/sc onstart参数是必需的。/sd(开始日期)参数是可选的,其默认值为当前日期。

12. 计划任务在用户登录时运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc onlogon [/sd StartDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示: "登录时"计划类型计划任务在任何用户登录到计算机时运行。在"登录时"计划类型中,/sc onlogon参数是必需的。/sd(开始日期)参数是可选的,其默认值为当前日期。

13. 计划任务在系统空闲时运行

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc onidle /i {1 - 999} [/sd StartDate] [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

提示: "空闲时"计划类型计划任务在/i参数指定的时间期间没有用户活动时运行。在

“空闲时”计划类型中，/sc onidle 参数和/i 参数是必需的。/sd(开始日期)是可选的，其默认值为当前日期。

14. 计划任务现在运行

schtasks 没有“现在运行”选项，但可以模拟该选项，方法是创建一个在较短时间内(如几分钟)只运行一次的任务。

该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc once [/st HH:MM] /sd MM/DD/YYYY [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

15. 计划任务以不同权限运行

可以计划各种类型的任务以备选账户的权限在本地计算机和远程计算机上运行。该命令的基本语法如下。

```
schtasks /create /tn TaskName /tr TaskRun /sc once [/st HH:MM] /sd MM/DD/YYYY [/it] [/ru {[Domain\]User [/rp Password] | System}] [/s Computer [/u [Domain\]User [/p Password]]]
```

该命令中各参数的含义如下。

(1) /ru 参数是必需的，而/rp 参数是可选的。

(2) /sc 参数指定日计划。

(3) /mo 参数指定时间间隔为 4 天。

(4) /s 参数提供远程计算机的名称。

(5) /u 参数指定在远程计算机上拥有计划任务权限的账户(Marketing 计算机上的 Admin01)。

(6) /ru 参数指定任务应以用户的非 Administrator 账户(Reskits 域中的 User01)权限运行。如果不使用/ru 参数，任务将以/u 指定的账户权限运行。

16. 计划任务以系统权限运行

各种类型的任务都可以用系统账户的权限在本地计算机和远程计算机上运行。除了特定计划类型所需的参数之外，/ru system(或/ru"")参数也是必需的，而/rp 参数无效。

提示： 系统账户没有交互式登录权限。用户无法看到以系统权限运行的程序或任务，也无法与之进行交互。/ru 参数确定运行任务的权限，而不是用来计划任务的权限。只有 Administrators 可以计划任务，与/ru 参数的值无关。

17. 计划任务运行多个程序

每个任务只能运行一个程序，但是可以创建一个运行多个程序的批处理文件，然后计划一个任务来运行这个批处理文件。

18. 计划任务在远程计算机上运行

要计划任务在远程计算机上运行，必须把任务添加到远程计算机的计划中。可以在远程计算机上计划各种类型的任务，但必须满足以下条件。

(1) 用户必须具有计划任务的权限。因此，必须以属于远程计算机上 Administrators 组成员的账户登录到本地计算机，或者必须使用/u 参数提供远程计算机管理员的凭据。

(2) 只有在本地计算机和远程计算机处于同一个域，或者本地计算机处于远程计算机域信任的域时，才能使用/u 参数。否则，远程计算机无法对指定的用户账户进行身份验证，

也无法验证该账户是否为 Administrators 组的成员。

(3) 用户必须具有足够的权限才能在远程计算机上运行。不同的任务要求不同的权限。默认情况下,任务以本地计算机当前用户的权限运行,或如果使用/u 参数,任务就以/u 参数指定的账户权限运行。但是,可以使用/ru 参数以另一个用户账户的权限或以系统权限运行任务。

2.6.2 更改任务属性——schtasks change

schtasks change 命令的主要功能如下。

(1) 更改一个或多个任务属性。

(2) 任务运行的程序(/tr)。

(3) 任务运行的用户账户(/ru)。

(4) 用户账户的密码(/rp)。

(5) 将仅交互属性添加到任务(/it)。

该命令的基本语法如下。

```
schtasks /change /tn TaskName [/s Computer [/u [Domain\] User [/p Password]]] [/ru {[Domain\] User | System}] [/rp Password] [/tr TaskRun] [/st StartTime] [/ri Interval] [{/et EndTime | /du Duration} [/k]] [/sd StartDate] [/ed EndDate] [/{ENABLE | DISABLE}] [/it] [/z]
```

该命令中各参数的含义如下。

(1) /tn TaskName:标识要更改的任务。输入任务名。

(2) /s Computer:指定远程计算机的名称或 IP 地址(带有或不带有反斜杠)。默认值是本地计算机。

(3) /u [Domain\] User:使用指定用户账户的权限运行该命令。默认值为本地计算机上当前用户的权限。指定的用户账户必须是远程计算机上 Administrators 组的成员。只有在远程计算机(/s)上更改任务时,/u 和/p 参数才有效。

(4) /p Password:指定在/u 参数中指定的用户账户的密码。如果使用/u 参数,但忽略/p 参数或密码参数,schtasks 将提示输入密码。只有使用/s 时,/u 和/p 参数才有效。

(5) /ru {[Domain\]User | System}:指定更改运行任务的用户账户。对于指定 Local System 账户,有效项为 NT AUTHORITY\SYSTEM 或 SYSTEM。在更改用户账户时,同时必须更改用户密码。如果某个命令包含/ru 参数,但不包含/rp 参数,schtasks 就会提示提供新密码。使用本地系统账户的权限运行任务不需要密码或不提示输入密码。

(6) /rp Password:为现有用户账户或/ru 参数指定的用户账户指定一个新密码。在本地系统账户中使用时,此参数会被忽略。

(7) /tr TaskRun:更改任务运行的程序。输入可执行文件、脚本文件或批处理文件的完全合格的路径和文件名。如果忽略该路径,schtasks 将假定文件在 Systemroot\System32 目录下。指定的程序替换任务运行的原始程序。

(8) /st StartTime:使用 24 小时时间格式 HH:MM 指定任务的开始时间,例如,值 14:30 相当于 12 小时时间格式的下午 2:30。

(9) /ri Interval:指定计划任务的重复间隔(以分钟计)。有效范围为 1～599940 (599940 分钟=9999 小时)。

（10）/et EndTime：使用 24 小时时间格式 HH:MM 指定任务的结束时间，例如，值 14:30 相当于 12 小时时间格式的下午 2:30。

（11）/du Duration：指定关闭 EndTime 或 Duration 的任务（如果指定的话）。

（12）/k 在/et 或/du 指定的时间停止任务运行的程序。如果没有/k，schtasks 在到达/et 或/du 指定的时间之后不再启动程序，但不会停止仍在运行的程序。此参数是可选的，并且仅对 MINUTE 或 HOURLY 计划有效。

（13）/sd StartDate：指定任务应运行的第一个日期。日期格式为 MM/DD/YYYY。

（14）/ed EndDate：指定任务应运行的最后一个日期。格式为 MM/DD/YYYY。

（15）/ENABLE：指定启用已计划的任务。

（16）/DISABLE：指定禁用已计划的任务。

（17）/it：指定仅在"运行方式"用户（运行任务的用户账户）登录到计算机时才运行已计划的任务。此参数不会影响使用系统权限运行的任务，也不会影响已经设置仅交互属性的任务。不能使用更改命令从任务中删除仅交互属性。默认情况下，在计划任务时或由/u 参数（如果使用该参数）指定账户时，"运行方式"用户将是本地计算机的当前用户。但是，如果该命令包含/ru 参数，"运行方式"用户则是由/ru 参数指定的账户。

（18）/z：指定在计划完成时删除任务。

2.6.3　立即运行计划任务——schtasks run

schtasks run 命令用于立即运行计划任务。run 操作忽略计划，但使用程序文件位置、用户账户和保存在任务中的密码立即运行任务。

该命令的基本语法如下。

```
schtasks /run /tn TaskName [/s Computer [/u [Domain\]User [/p Password]]]
```

该命令中各参数的含义如下。

（1）/tn TaskName：该参数是必需的。标识启动程序的任务。

（2）/s Computer：指定远程计算机的名称或 IP 地址（带有或不带有反斜杠）。默认设置为本地计算机。

（3）/u [Domain\] User：使用指定用户账户的权限运行该命令。默认情况下，使用本地计算机当前用户的权限运行该命令。指定的用户账户必须是远程计算机上 Administrators 组的成员。只有使用/s 时，/u 和/p 参数才有效。

（4）/p Password：指定在/u 参数中指定的用户账户的密码。如果使用/u 参数，但忽略/p 参数或密码参数，schtasks 将提示输入密码。只有使用/s 时，/u 和/p 参数才有效。

2.6.4　停止由任务启动的程序——schtasks end

schtasks end 命令用于停止由任务启动的程序。

该命令的基本语法如下。

```
schtasks /end /tn TaskName [/s Computer [/u [Domain\]User [/p Password]]]
```

该命令中各参数的含义如下。

(1) /tn TaskName：该参数是必需的。标识启动程序的任务。

(2) /s Computer：指定远程计算机的名称或 IP 地址。默认设置为本地计算机。

(3) /u [Domain\] User：使用指定用户账户的权限运行该命令。默认情况下，使用本地计算机当前用户的权限运行该命令。指定的用户账户必须是远程计算机上 Administrators 组的成员。只有使用/s 时，/u 和/p 参数才有效。

(4) /p Password：指定在/u 参数中指定的用户账户的密码。如果使用/u 参数，但忽略/p 参数或密码参数，schtasks 将提示输入密码。只有使用/s 时，/u 和/p 参数才有效。

2.6.5 删除计划任务——schtasks delete

schtasks delete 命令用于删除计划任务。

该命令的基本语法如下。

```
schtasks /delete /tn {TaskName | *} [/f] [/s Computer [/u [Domain\]User [/p Password]]]
```

该命令中各参数的含义如下。

(1) /tn {TaskName | *}：该参数是必需的。标识要删除的任务。值描述：TaskName 删除已命名任务；* 删除计算机上的所有计划任务。

(2) /f：阻止确认消息。不警告就删除任务。

(3) /s Computer：指定远程计算机的名称或 IP 地址(带有或不带有反斜杠)。默认设置为本地计算机。

(4) /u [Domain\] User：使用指定用户账户的权限运行该命令。默认情况下，使用本地计算机当前用户的权限运行该命令。指定的用户账户必须是远程计算机上 Administrators 组的成员。只有使用/s 时，/u 和/p 参数才有效。

(5) /p Password：指定在/u 参数中指定的用户账户的密码。如果使用/u 参数，但忽略/p 参数或密码参数，schtasks 将提示输入密码。只有使用/s 时，/u 和/p 参数才有效。

2.6.6 显示计划运行的任务——schtasks query

schtasks query 命令用于显示计划在计算机上运行的任务。

该命令的基本语法如下。

```
schtasks [/query] [/fo {TABLE | LIST | CSV}] [/nh] [/v] [/s Computer [/u [Domain\]
User [/p Password]]]
```

该命令中各参数的含义如下。

(1) [/query]：操作名称可选。输入不带任何参数的 schtasks 执行查询。

(2) /fo {TABLE| LIST| CSV}：指定输出格式。TABLE 为默认值。

(3) /nh：忽略表格显示中的列标题。此参数对 TABLE 和 CSV 输出格式有效。

(4) /v：将任务的高级属性添加到显示中。使用/v 的查询格式应该设置为 LIST 或 CSV。

（5）/s Computer：指定远程计算机的名称或 IP 地址（带有或不带有反斜杠）。默认设置为本地计算机。

（6）/u [Domain\] User：使用指定用户账户的权限运行该命令。默认情况下，使用本地计算机当前用户的权限运行该命令。指定的用户账户必须是远程计算机上 Administrators 组的成员。只有使用/s 时，/u 和/p 参数才有效。

（7）/p Password：指定在/u 参数中指定的用户账户的密码。如果使用/u，但忽略/p 或密码参数，schtasks 将提示输入密码。只有使用/s 时，/u 和/p 参数才有效。

2.7　本地用户和用户组的管理

本地用户和用户组都是针对本地计算机而言的，与域用户相对应。通常情况下，安装操作系统的同时就已经创建了一个本地用户账户，该用户账户隶属于管理员组，享有较多的系统操作和管理权限。使用过程中，还可以根据需要以系统管理员的名义创建多个本地用户和用户组，分别赋予不同的操作权限即可。

2.7.1　创建本地用户账户

在将 Windows Server 2008 计算机升级到域控制器之前，可以使用“计算机管理”控制台来创建本地用户账户。

（1）依次选择“开始”→“管理工具”→“计算机管理”命令，显示图 2-52 所示的“计算机管理”控制台窗口。

（2）在左侧控制台树中，依次展开“系统工具”→“本地用户和组”→“用户”目录，在右侧的空白窗口中右击，在快捷菜单中选择“新用户”命令，显示图 2-53 所示的“新用户”对话框。在“用户名”文本框中输入欲创建的用户名，在“密码”和“确认密码”文本框中输入为新用户设置的密码。需要注意的是，这里所设置的密码必须满足密码要求。在下方还有 4 个复选框，含义分别如下。



图 2-52　“计算机管理”窗口



图 2-53　“新用户”对话框

①"用户下次登录时须更改密码:如果选中此复选框,则当使用该用户名在下次登录时,Windows 会提示用户更改密码。

②"用户不能更改密码:如果选中此复选框,则用户将一直使用在"密码"文本框中设置的密码。

③"密码永不过期:如果选中此复选框,则在使用此用户登录计算机的过程中,密码将永久有效。

④"账户已禁用:如果选中此复选框,则此用户账户将不能再用来登录计算机。

(3) 单击"创建"按钮,完成一个用户的创建。重复操作,可添加多个用户。最后,单击"关闭"按钮返回"计算机管理"窗口即可。

在创建用户的过程中,需要注意如下事项。

(1) 用户名不能与被管理的计算机的主机名以及其他用户或组名相同。用户名最多可以包含 20 个大写或小写字符,但不能包含"、/、\、[、]、:、;、|、=、,、+、*、?、<、>字符。用户名也不能只由句点(.)和空格组成。

(2) 在"密码"和"确认密码"文本框中,可以输入包含不超过 127 个字符的密码。但是,如果网络中包含运行 Windows 95 或 Windows 98 的计算机,建议使用不超过 14 个字符的密码,如果密码过长,可能无法从这些计算机登录网络。

(3) 创建用户时,"用户下次登录时须更改密码"和"用户不能更改密码"、"密码永不过期"复选框不能同时选中。

2.7.2 设置本地用户账户的属性

用户账户不只包括用户名、密码等信息,为了管理和使用的方便,还应包括用户属于的用户组、用户配置文件、用户的拨入权限、终端权限设置等,从而使管理员对用户的管理更加完善。

在"本地用户和组"的右侧窗口中,双击某用户,即可显示该用户属性对话框,如图 2-54 所示。



图 2-54 修改用户属性

其中,"常规"、"隶属于"、"配置文件"、"拨入"选项卡中是用户的普通属性,"远程控制"、"终端服务配置文件"、"环境"、"会话"选项卡中是有关终端服务的用户属性,只有在安装了终端服务之后才会出现。

1. "常规"选项卡

在"常规"选项卡中,与创建用户时的大部分选项相同,除了在创建用户时的 4 个复选框之外,还包括一个"账户已锁定"复选框,这一复选框是只有在用户被锁定时(用户输入密码的错误次数达到锁定要求时),可以在"常规"选项卡解除锁定。

2. "隶属于"选项卡

在"隶属于"选项卡中,列出了当前用户属于哪个用户组。为了管理的方便,通常都是对用户组进行权限的分配与设置,用户属于哪一个用户组,就具有相应用户组的权限。新创建的默认用户组是 Users,如图 2-55 所示,管理员可以通过单击"添加"按钮,将用户添加到某一个或几个用户组中,也可以单击"删除"按钮将用户从一个或几个用户组中删除。

添加用户组的操作如下。

(1) 单击“添加”按钮，显示“选择组”对话框。单击“高级”按钮然后单击“立即查找”按钮，开始搜索当前计算机上的所有用户组并在“搜索结果”列表中显示，如图 2-56 所示。使用 Ctrl 键或 Shift 键，可以选择多个用户组。



图 2-55　“隶属于”选项卡



图 2-56　选择用户组

(2) 连续单击“确定”按钮，返回到用户属性对话框即可。

3. “配置文件”选项卡

在“配置文件”选项卡中，可以设置用户的配置文件夹路径和选择用户的登录脚本以及用户的主文件夹，如图 2-57 所示。

在设置登录脚本时，注意如下问题。

(1) 登录脚本可能包含恶意命令。建议在向用户指派登录脚本之前，先熟悉脚本的内容。

(2) 存储在本地计算机上的登录脚本，仅适用于登录到本地计算机的用户。

(3) 本地登录脚本必须存储在指定共享文件夹(Netlogon)或者该共享文件夹的子文件夹中。如果该文件夹不存在，必须手动创建该文件夹并设置为共享。要指定 Netlogon 文件夹的子文件夹中存储的登录脚本，必须在文件名前面使用该文件夹的相对路径。例如，要将存储在\\ComputerName\Netlogon\FolderName 中的登录脚本 Startup. bat 指派给本地用户，在“登录脚本”文本框中输入 FolderName\Startup. bat。



图 2-57　“配置文件”选项卡

在设置主文件夹时，注意如下问题。

(1) “我的文档”提供了到主文件夹的一个便捷替代方式，但并不能替代这些主文件夹。每个用户在启动卷中都有一个对应的“我的文档”文件夹。要确定用户的“我的文档”文件夹的位置，作为该用户登录，单击“开始”按钮，右击“我的文档”选项，选择“属性”命令，查看在

“目标文件夹”选项卡上指定的位置。

(2) 要更改“我的文档”文件夹的目标文件夹位置，单击“开始”按钮，右击“我的文档”选项，再选择“属性”命令。在“目标文件夹”选项卡的“目标文件夹位置”文本框中输入新的文件夹位置。

(3) 如果未指派主文件夹，系统将为用户账户指派一个默认的本地主文件夹(在系统盘根目录下，也就是安装操作系统文件的初始目录)。

(4) 要指定主文件夹的网络路径，首先必须创建共享资源，然后设置允许用户访问的足够权限。

4. “拨入”选项卡

在“拨入”选项卡中，可以进行用户的远程访问相关的权限设置，如图 2-58 所示。远程访问是网络服务器管理的常用方式，例如 VPN 接入方式。在“拨入”选项卡中可以对远程管理用户的操作权限进行设置。

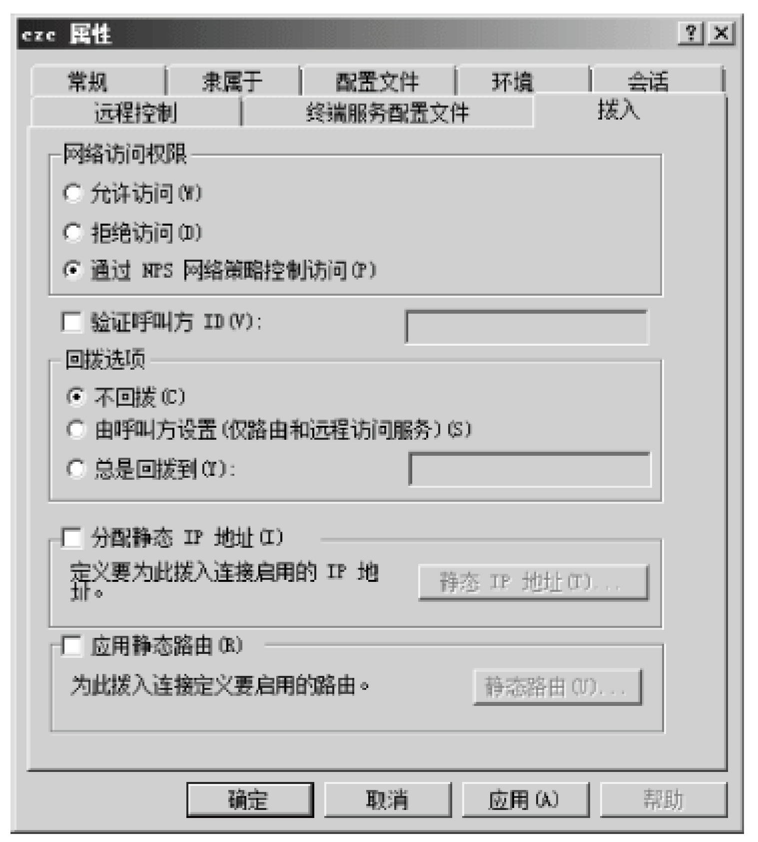


图 2-58 “拨入”选项卡

2.7.3 修改用户名或密码

通常情况下，为了网络管理的安全，需要将系统管理员账户(Administrator)进行重命名。另外，网络管理或其他应用过程中(如用户对为其设置的用户名不满意时)，也需要修改用户账户名称。当用户忘记登录密码时，可以使用具有管理员身份的用户账户登录计算机，对忘记密码的用户设置新的密码。

修改用户名的操作非常简单，在“计算机管理”窗口的“用户”列表中右击想要更名的用户账户，选择“重命名”命令，并输入新的用户名即可。

修改用户账户密码的具体操作步骤如下。

(1) 在“计算机管理”窗口中，右击想要修改密码的用户，以用户 czc 为例，在快捷菜单中选择“设置密码”命令，显示图 2-59 所示的警告对话框。

(2) 单击“继续”按钮，显示图 2-60 所示的“为 czc 设置密码”对话框。在“新密码”和“确认密码”文本框中输入新设置的密码。

(3) 单击“确定”按钮，显示图 2-61 所示的“本地用户和组”对话框，提示密码修改成功。

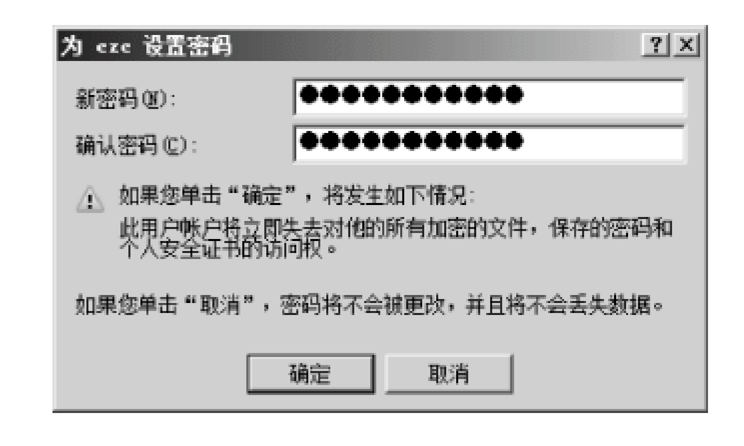


图 2-60 输入新设置的密码

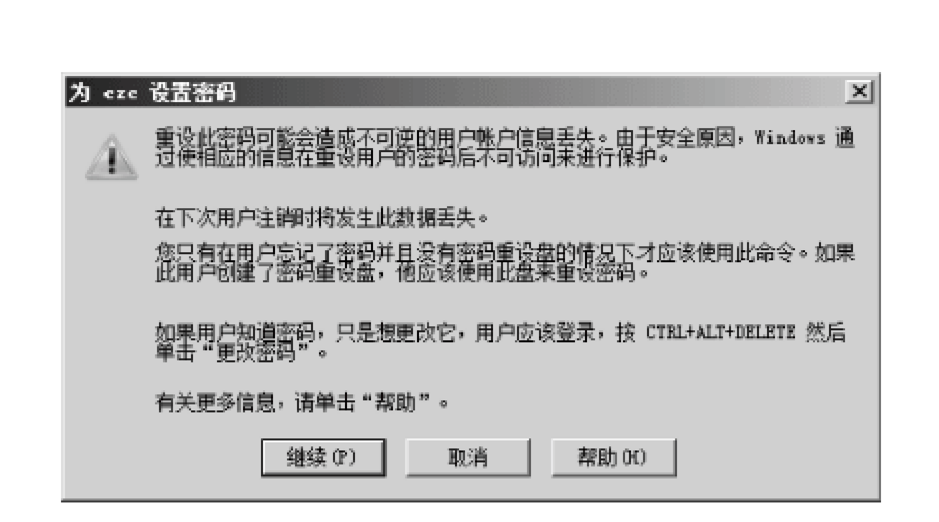


图 2-59 警告对话框



图 2-61 成功修改用户密码

(4) 单击“确定”按钮,关闭该对话框即可。

注意:在修改用户名后,新修改的用户名保留原用户名的密码等相关信息,只是登录用户名做了修改。

2.7.4 默认的本地用户组

为了管理的方便,Windows Server 2008 已经创建了一些本地用户组,默认的用户组主要用来完成日常的管理工作。默认的用户组的权限如表 2-5 所示。

表 2-5 Windows Server 2008 默认的用户组的权限

组	描 述	默认用户权利
Administrators	该组的成员具有对服务器的完全控制权限,并且可以根据需要向用户指派用户权利和权限。管理员账户也是默认成员。当该服务器加入域中时,组会自动添加到该组中。由于该组可以完全控制服务器,所以向该组添加用户时应谨慎	从网络访问此计算机;调整某个进程的内存配额;允许本地登录;允许通过终端服务登录;备份文件和目录;跳过遍历检查;更改系统时间;更改时区;创建页面文件;创建全局对象;创建符号链接;调试程序;从远程系统强制关机;身份验证后模拟客户端;提高日程安排的优先级;加载和卸载设备驱动程序;作为批处理作用登录;管理审核和安全日志;修改固件环境变量;执行卷维护任务;配置单一进程;配置系统性能;从扩展坞中取出计算机;恢复文件和目录;关闭系统;取得文件或其他对象的所有权
Backup Operators	该组的成员可以备份和还原服务器上的文件,而不管保护这些文件的权限。这是因为执行备份任务的权利要高于所有文件权限。他们不能更改安全设置	通过网络访问此计算机;允许本地登录;备份文件和目录;跳过遍历检查;作为批处理登录;还原文件和目录;关闭系统
Cryptographic Operators	已授权此组的成员招待加密操作	没有默认的用户权利
Distributed COM Users	允许此组的成员在计算机上启动、激活和使用 DCOM 对象	没有默认的用户权利
Guests	该组的成员拥有一个在登录时创建的临时配置文件,在注销时,该配置文件将被删除。来宾账户(默认情况下已禁用)也是该组的默认成员	没有默认的用户权利
IIS_IUSRS	这是 Internet 信息服务(IIS)使用的内置组	没有默认的用户权利
Network Configuration Operators	该组的成员可以更改 TCP/IP 设置并更新和发布 TCP/IP 地址。该组中没有默认的成员	没有默认的用户权利
Performance Monitor Users	该组的成员可以从本地服务器和远程客户端监视性能计数器,而不用成为 Administrators 或 Performance Log Users 组的成员	没有默认的用户权利

续表

组	描　述	默认用户权利
Performance Log Users	该组的成员可以从本地服务器和远程客户端管理性能计数器、日志和警报，而不用成为 Administrators 组的成员	没有默认的用户权利
Power Users	默认情况下，该组的成员拥有不高于标准用户账户的用户权利或权限。在早期版本的 Windows 中，Power Users 组专门为用户提供特定的管理员权利和权限执行常见的系统任务。在此版本 Windows 中，标准用户账户具有执行最常见配置任务的能力，例如更改时区。对于需要与早期版本的 Windows 相同的 Power User 权利和权限的旧应用程序，管理员可以应用一个安全模板，此模板可以启用 Power Users 组，以假设具有与早期版本的 Windows 相同的权利和权限	没有默认的用户权利
Remote Desktop Users	该组的成员可以远程登录服务器	允许通过终端服务登录
Replicator	Replicator 组支持复制功能。Replicator 组的唯一成员应该是域用户账户，用于登录域控制器的“复制程序”服务。不能将实际用户的用户账户添加到该组中	没有默认的用户权利
Users	该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机。默认情况下，Domain Users、Authenticated Users 以及 Interactive 组是该组的成员。因此，在域中创建的任何用户账户都将成为该组的成员	从网络访问此计算机；允许本地登录；忽略遍历检查；更改时区；增加进程工作集；从扩展坞中取出计算机；关闭系统
提供远程协助帮助程序	该组的成员可以向此计算机用户提供远程协助	没有默认的用户权利

2.7.5 向组中添加用户

将用户添加到组，主要是用于将大批用户添加到一个用户组。如果只是提升一个用户的权限，可以在用户属性中选择添加一个或多个用户组。这里以向 Administrators 用户组中添加用户账户进行介绍。

(1) 在“计算机管理”窗口中，右击 Administrators 用户组，在快捷菜单中选择“属性”命令，显示“Administrators 属性”对话框。

(2) 单击“添加”按钮，显示图 2-62 所示的“选择用户”对话框。

(3) 单击“高级”按钮，显示“选择用户”的高级功能。单击“立即查找”按钮，将查找系统中所有的用户，如图 2-63 所示。从“搜索结果”列表中，选择将要添加到 Administrators 的用户账户。



图 2-62 “选择用户”对话框



图 2-63 选择用户

(4) 连续单击“确定”按钮，返回到“Administrators 属性”对话框，用户已经添加到该组中，如图 2-64 所示。

(5) 单击“确定”按钮，保存返回“计算机管理”窗口即可。

2.7.6 创建本地用户组

通常情况下，系统默认的用户组已经能够满足需要。但是，为了管理更加方便，或者完成其他的管理，或者一些特殊的情况下，还需要创建一些用户组。

从“计算机管理”窗口中，依次展开“本地用户和组”→“组”目录，在右边的空白窗格中右击，在快捷菜单中选择“新建组”命令，显示图 2-65 所示的“新建组”对话框。在“组名”和“描述”文本框中分别输入组名及描述信息，单击“创建”按钮即可以完成创建。



图 2-64 “Administrators 属性”对话框



图 2-65 “新建组”对话框

2.8 网络配置与协议管理

服务器是整个网络的核心，但接入网络之前必须先对服务器进行必要的网络设置，如安装网卡驱动程序、设置 IP 地址信息等。Windows Server 2008 系统中已经内置了大部分网

卡的驱动程序，默认可以自动安装，同时创建网络适配器对应的网络连接，管理员只需进行简单配置即可。

2.8.1 设置 IP 地址信息

设置 IP 地址信息的步骤如下。

(1) 在“控制面板”窗口中双击“网络和共享中心”图标，打开图 2-66 所示的“网络和共享中心”窗口。

(2) 单击“查看状态”按钮，显示图 2-67 所示的“本地连接 状态”对话框，显示当前网卡的状态。

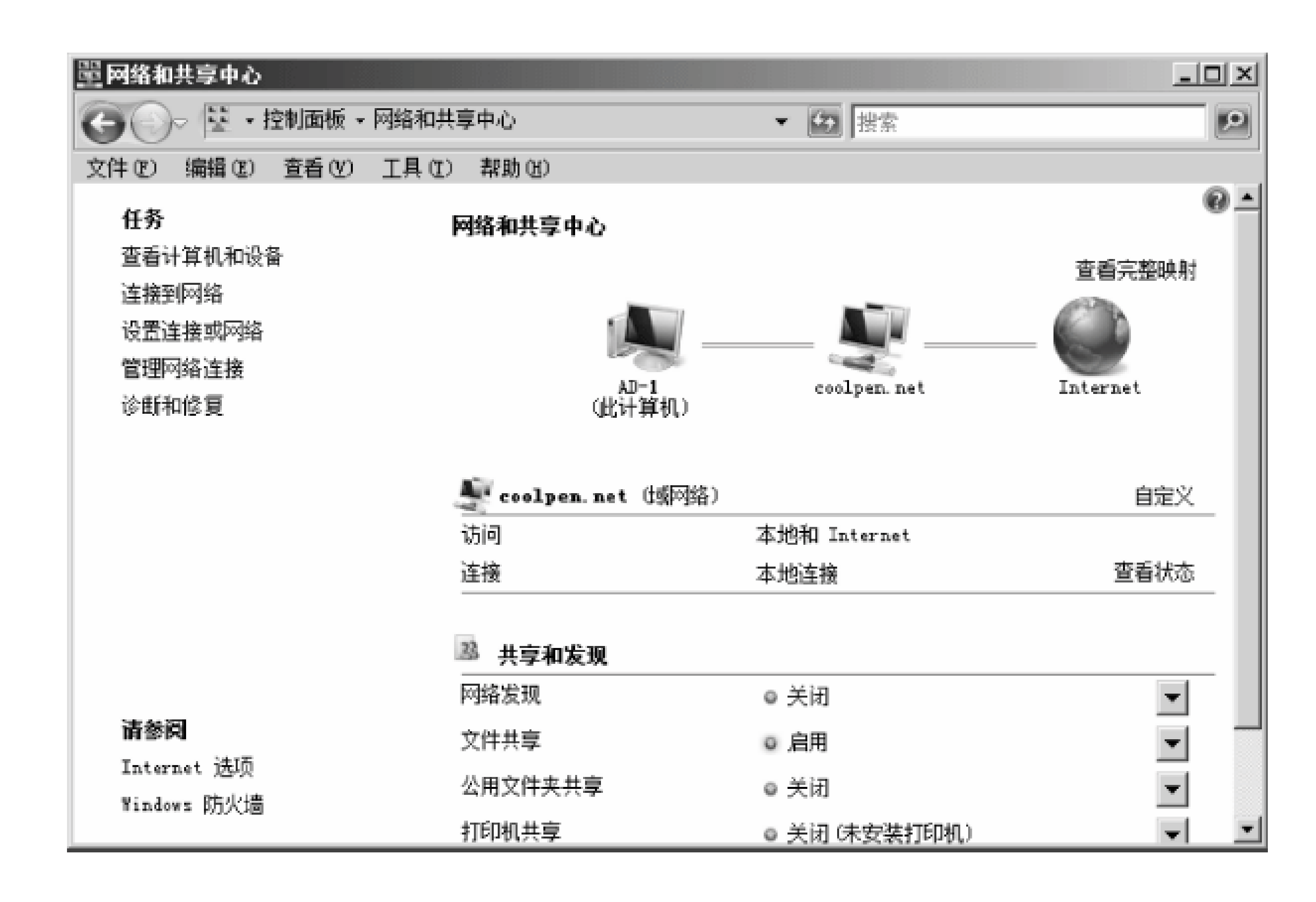


图 2-66 “网络和共享中心”窗口

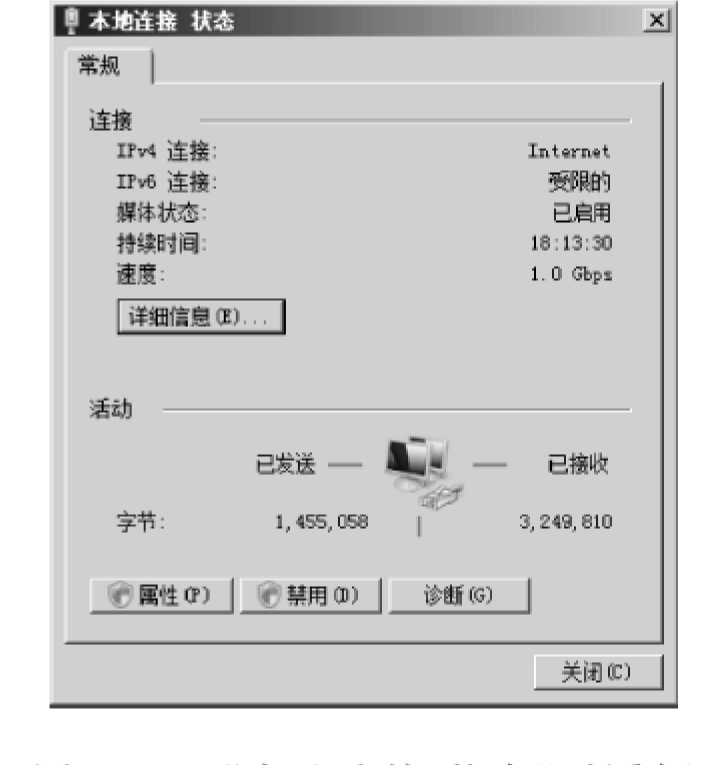


图 2-67 “本地连接 状态”对话框

(3) 单击“属性”按钮，显示图 2-68 所示的“本地连接 属性”对话框，在列表中选中“Internet 协议版本 4(TCP/IPv4)”复选框。

(4) 单击“属性”按钮，显示图 2-69 所示的“Internet 协议版本 4(TCP/IPv4) 属性”对话框。分别选中“使用下面的 IP 地址”和“使用下面的 DNS 服务器地址”单选按钮，并分别输入该计算机分配的 IP 地址、子网掩码、默认网关和 DNS 服务器的 IP 地址。



图 2-68 “本地连接 属性”对话框

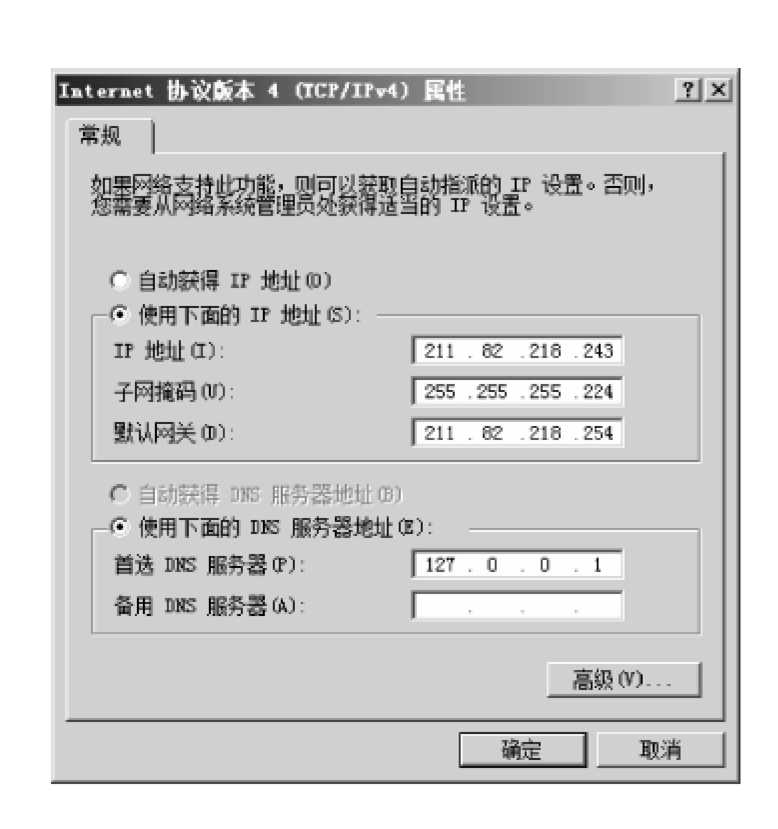


图 2-69 “Internet 协议版本 4(TCP/IPv4) 属性”对话框

(5) 连续单击“确定”按钮,保存设置即可。

2.8.2 知识链接:IP 地址信息

计算机或网络设备的 IP 地址信息由 IP 地址、子网掩码、默认网关和 DNS 服务器地址 4 部分组成。

1. IP 地址

网络使用的合法 IP 地址由提供 Internet 接入的服务商(ISP)分配,私有 IP 地址则可以由网络管理员自由分配。需要注意的是,网络内部所有计算机的 IP 地址都不能相同,否则会发生 IP 地址冲突,导致网络通信失败。

另外,IP 地址可以是静态或动态分配。不过,对于网络服务器而言,由于必须提供静态的 IP 地址才能方便地让网络用户找到,因此,通常情况下,不考虑为网络服务器动态分配 IP 地址。

所谓私有地址(Private Address)属于非注册地址,专门为组织机构内部使用。这些 IP 地址不能直接访问 Internet,也不能被 Internet 所访问,所以,即使被不同的网络使用,也不会导致 IP 地址冲突。

可供使用的私有 IP 地址包括以下几类。

(1) A 类:10.0.0.0~10.255.255.255。

(2) B 类:172.16.0.0~172.31.255.255。

(3) C 类:192.168.0.0~192.168.255.255。

2. 子网掩码

子网掩码用于划分不同的网络,从而判断自己所处的网络,以及与对方是否处于同一网络。如果使用的内部保留 IP 地址,那么,通常可以采用默认的子网掩码。如果是采用合法的 IP 地址,则要通过设置变长子网掩码的方式合理划分子网。

各类 IP 地址默认的子网掩码分别如下。

(1) A 类:255.0.0.0。

(2) B 类:255.255.0.0。

(3) C 类:255.255.255.0。

提示:有关 IP 地址和子网掩码的详细内容,参见其他技术资料。

3. 默认网关

所谓网关(Gateway)是一个网络连接到另一个网络的“关口”。例如,跟同一间办公室的同事聊天,可以站起来直接跟他讲,而与另一间办公室的同事谈事情,就必须从门口走出去。事实上,无论与其他哪间办公室的同事面对面交流,都必须走出自己办公室的门口。而所谓默认网关,就是指将对其他网络的访问发送到哪个 IP 地址,即访问其他网络所必经的“关口”。

只有设置了网关,TCP/IP 协议才能实现不同网络之间的相互通信。而作为网关的 IP 地址应当是具有路由功能的设备的 IP 地址,如路由器、宽带路由器、代理服务器、三层交换机等的局域网 IP 地址。

提示:当主机访问其他网络时,只需将数据包发给默认网关就不用管了,后续的一切工作都由这个网关来负责处理。在大中型网络中,每个 VLAN 使用的默认网关都不相同。

4. DNS 服务器

网络中的计算机之间是通过 IP 地址进行通信的。但是,IP 地址既长又枯燥,非常难以记忆。于是,人们便发明了有意义且易记的域名,然后,再借助 DNS 服务将域名转换为 IP 地址。这样,当访问某个网站时,只需输入易记的域名就行了。如果局域网中没有提供 DNS 服务,那么,DNS 服务器的 IP 地址应该是 ISP 的 DNS 服务器。

例如,当访问清华大学网站时,只须输入其域名“http://www.tsinghua.edu.cn/”即可。其中,www 表示提供 Web 服务,tsinghua 是清华的英文写法,edu 表示教育机构,cn 表示中国。显然,记忆这个域名比其 IP 地址“166.111.4.100”容易得多。

如果局域网自己提供了 DNS 服务,那么,DNS 服务器的 IP 地址就是内部 DNS 服务器的 IP 地址。但目前使用最多的是公网上的 DNS 服务器,例如,河北省公网的 DNS 服务器的 IP 地址为 202.99.160.68 和 202.99.166.4。

2.8.3 网卡的禁用与启用

目前,服务器通常都标配有两个网络适配器接口。因此,除非采用 EtherChannel 技术将两块网卡绑定在一起使用,实现带宽倍增和负载均衡;否则,应当将其中一块网卡禁用,以避免可能会导致无法正常通信的故障。因此,建议管理员仅在必要的时候启用备用网卡网络连接,不用时则将其禁用。

提示:代理服务器和软件路由服务器除外,因为它们的两块网卡分别连接至内网和外网,需要同时启用,才能实现代理和路由服务。另外,在实现服务器群集时,每台服务器也需要使用两块网卡,分别用于提供网络服务和负载均衡。

1. 网卡的禁用

禁用网卡后对应网络连接将停止工作,但是其配置信息将不会消失或还原。用户可以通过如下几种方法禁用网卡。

(1)“网络连接”窗口

在“网络连接”窗口中,右击想要禁用的网卡对应的网络连接,并在快捷菜单中选择“禁用”命令即可直接禁用该连接,如图 2-70 所示。稍等片刻即可发现该网络连接图标已经呈灰色显示,表示已经禁用。

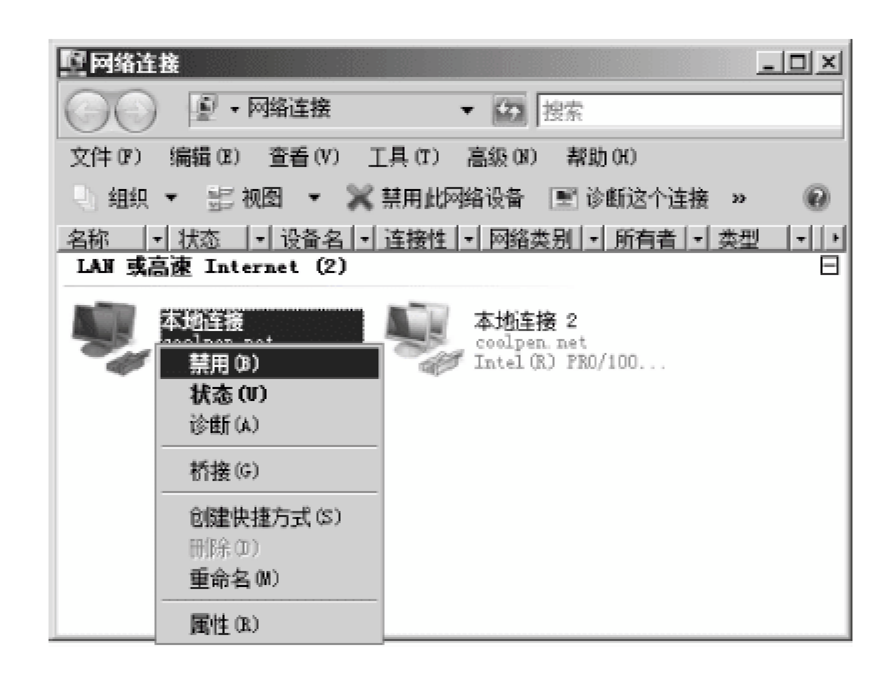


图 2-70 “网络连接”窗口

(2)设备管理器

所有硬件设备的禁用或启用都可以通过设备管理器来完成。打开“设备管理器”窗口,如图 2-71 所示,当前计算机上已安装的所有硬件设备信息都会显示在这里。展开“网络适配器”目录,即可看到已安装的所有网卡,右击想要禁用的网卡,选择“禁用”命令即可将其禁用。成功禁用后该网卡对应的图标上会看到一个“红叉”标记。

2. 网卡的启用

必要的时候可以将处于禁用状态的网卡重新启用,此时网卡配置信息会保持不变,可立即应用。启用网卡同样有多种方法,和网卡的禁用操作恰恰相反,即无论采用哪种方法只需选择对应的“启用”命令即可,此处不再赘述。

2.8.4 创建网络连接

如果只进行局域网内部计算机之间的资源共享，则只做上述简单配置即可。但是很多情况下服务器需要连接到其他局域网或远程网络，如 Internet、公司网络等，此时，还需要创建一个专用的网络连接，必要的情况下还需要安装专用连接设备。

（1）打开"网络和共享中心"窗口，在左侧中单击"设置连接或网络"链接，显示图 2-72所示的"设置连接或网络"向导。在列表中选中"连接到 Internet"选项。

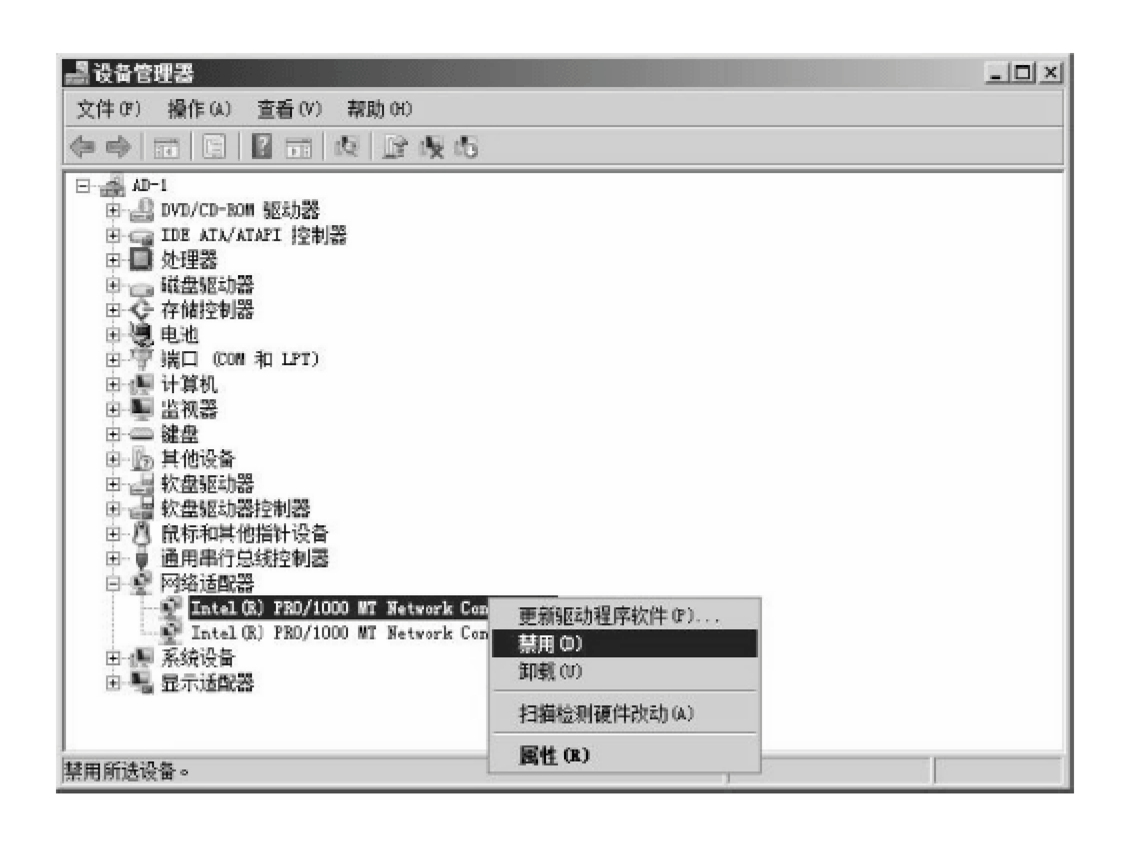



图 2-71 计算机管理



图 2-72 "设置连接或网络"向导窗口

（2）单击"下一步"按钮，显示"您想如何连接"窗口。

（3）单击"宽带（PPPoE）"按钮，显示图 2-73 所示的"输入您的 Internet 服务提供商（ISP）提供的信息"窗口。分别在"用户名"和"密码"文本框中输入网络提供商所分配的用户名及密码。在"连接名称"文本框中输入该连接所显示的名称。另外，如果选中"记住此密码"复选框，在下次使用时不用再重复输入该密码。如果选中"允许其他人使用此连接"复选框，则允许所有用户使用该连接。



图 2-73 "输入您的 Internet 服务提供商(ISP)提供的信息"窗口

（4）单击“连接”按钮，可立即连接到网络，连接成功后显示图 2-74 所示的“到 Internet 的连接可以使用”窗口。

（5）单击“关闭”按钮，即可完成整个 Internet 连接的建立，如图 2-75 所示。如果以后需要创建或修改其他配置，可以随时启动连接向导。




图 2-74 “到 Internet 的连接可以使用”窗口



图 2-75 “连接 宽带连接”对话框

对于通过局域网接入 Internet 连接的用户而言，在 Windows 操作系统下不必建立新的连接，局域网连接是 Windows 自动建立的。当需要创建多个用于访问不同网络的连接时，可以直接复制已经创建好的网络连接，然后再简单更改名称、基本设置信息即可。

2.9 远程管理

众所周知，在网络中，网络服务器和计算机因为功能的不同，通常位于网络的不同位置，这在很大程度上增加了网络管理的难度。如果单纯地依靠人力来完成，显然是比较困难的。因此，使用远程监视和控制工具是提高网络管理效率最有效的方法。

2.9.1 启用服务器的远程桌面功能

如果欲使用远程桌面管理服务器，首先必须在服务器上启用远程桌面功能。具体操作步骤如下。

（1）右击“计算机”图标，并在快捷菜单中选择“属性”命令，打开“系统”窗口。

（2）在“任务”选项区域中，单击“高级系统设置”按钮，显示图 2-76 所示的“系统属性”对话框。在“远程桌面”选项区域中，根据需要选择所要使用的远程桌面级别。

① 不允许连接到这台计算机：禁用远程桌面。

② 允许运行任意版本远程桌面的计算机连接（较不安全）：任意可以连接到这台服务器的计算机均可使用远程桌面管理该服务器。

③ 只允许运行带网络级身份验证的远程桌面的计算机连接（更安全）：只允许带网络级身份验证的计算机连接到该服务器，该连接方式更能保证服务器的安全。

（3）单击“选择用户”按钮，显示图 2-77 所示的“远程桌面用户”对话框，单击“添加”按钮，将允许连接到该服务器的用户添加到允许列表中。需要注意的是，默认情况下管理员 Administrator 已经拥有管理权限。



图 2-76　“系统属性”对话框

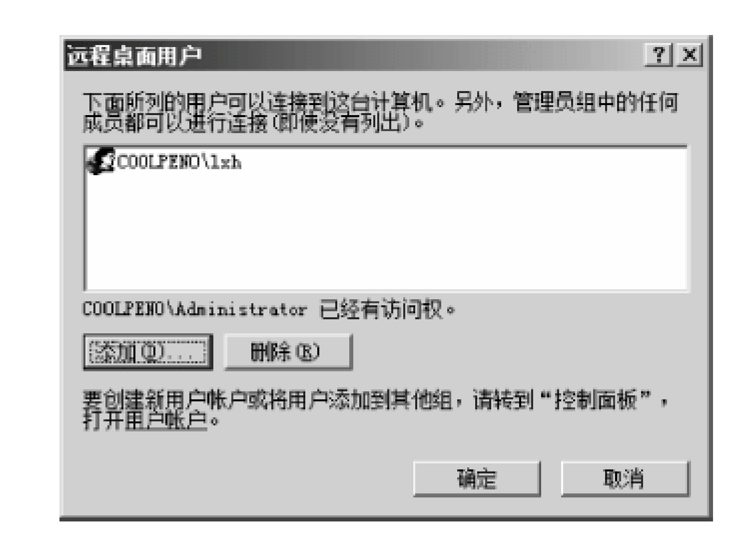


图 2-77　“远程桌面用户”对话框

(4) 依次单击“确定”按钮，保存设置即可。

2.9.2　远程桌面连接程序——MSTSC

MSTSC(Microsoft Remote Desktop Connection)是一款实用的 Windows 桌面连接程序。可以帮助用户创建到终端服务器或其他远程主机的连接，将远程主机的桌面映射连接到本地计算机桌面。当连接到远程服务器控制台连接时，不需要任何其他用户事先登录到该控制台连接。即使没有人登录到该控制台，也可以像实际位于该控制台前一样登录。

实例：连接到服务器的控制台会话。

在命令提示符窗口中输入如下命令。

```
mstsc /console
```

按 Enter 键执行，显示图 2-78 所示的运行结果。



图 2-78　连接到服务器

在“计算机”文本框中输入远程计算机的 IP 地址，单击“连接”按钮，即可连接到远程桌面。

小知识：单击“选项”按钮，可以根据需要设置远程连接的属性。

2.9.3　知识链接：MSTSC 命令

MSTSC 命令的基本语法格式如下。

```
mstsc.exe {ConnectionFile | /v:ServerName[:Port]} [/console] [/f] [/w:Width/h:Height]
mstsc.exe /edit"ConnectionFile"
mstsc.exe /migrate
```

该命令中各参数的含义如下。

(1) /ConnectionFile：指定用于连接的.rdp 文件的名称。

(2) /v：ServerName[:Port]：指定要连接的远程计算机和(可选)端口号。

(3) /console：连接到指定的 Windows Server 2003 家族操作系统的控制台会话。

(4) /f：在全屏模式下启动“远程桌面”连接。

(5) /w：Width /h：Height：指定“远程桌面”屏幕的大小。

(6) /edit " ConnectionFile "：打开指定的.rdp 文件进行编辑。

(7) /migrate：将使用“客户端连接管理器”创建的旧的连接文件迁移到新的.rdp 连接文件中。

注意：

(1) 必须是要连接的服务器上的管理员才能创建远程控制台连接。

(2) 对于每个用户来说，默认的.rdp 都作为隐藏文件存储在“我的文档”中。默认情况下，用户创建的.rdp 文件存储在“我的文档”中。

习题

1. 简述 RAID 常用级别的特点，以及各级别的适用环境。
2. 简述 PowerShell 的功能。
3. IP 地址信息由哪几部分组成？

实验：设置 Windows Server 2008 RAID 5

实验目的：

熟练掌握 Windows Server 2008 系统中设置 RAID 5 的方法。

实验内容：

在拥有 3 块以上磁盘的 Windows Server 2008 系统中，创建 RAID 5 卷。

实验步骤：

(1) 打开“磁盘管理”窗口。

(2) 启动欢迎使用新建 RAID 5 卷向导。

(3) 添加磁盘并设置卷大小。

(4) 格式化 RAID 5 卷。

第 3 章 chapter 3

Windows 系统性能管理

服务器性能的好坏直接影响其为网络提供服务的质量，如果服务器长期处于高负荷的工作状态下，将很难保证其服务质量。尤其是网络中的重要服务器更需要保证其具有高可用性，例如域控制器、文件服务器等。因此，在网络管理过程中，为了保证 Windows 系统的性能，必须对系统进行必要的设置和监视。

3.1 Windows 系统性能规划

高性能的服务器是实现所有功能的基础，一个性能低下的服务器是无法达到用户要求的，因此，保证系统的性能是保证服务器提供优质服务的前提。

3.1.1 项目背景

通常情况下，新版本的服务器操作系统比早期的服务器操作系统，对服务器硬件的利用程度要高，其实这也是服务器软件技术的发展所需要的。为了能够最大限度地提高系统性能，需要管理员掌握一些必要的优化系统性能的方式、方法。

3.1.2 项目需求

通常情况下，影响系统性能的因素包括如下几方面的内容。

(1) 操作系统软件。合理地选择操作系统程序也是提高系统性能的方法之一。

(2) 优化系统性能。影响系统性能的因素包括多个方面的内容，为了能够提高系统性能，需要将其中影响系统性能的不必要的项目关闭，或进行相应的调整。

(3) 为了能够清楚地了解服务器的可靠性和性能，需要管理员时常进行监视。

3.1.3 解决方案

针对于当前网络项目中的 Windows 系统性能管理要求，可使用如下解决方案。

(1) 选择 Server Core 操作系统，Server Core 不具有图形界面，采用纯命令操作，类似于 Linux 和 UNIX。由于 Server Core 安装的组件少，只有系统核心基础服务，因此，降低了被攻击的可能性，安全性更加可靠，稳定性也更高。不过，Server Core 安装以后需要使用各种命令进行管理，这就需要网络管理员掌握一定的命令使用方式。

(2) 关于系统性能优化，可通过删除不必要的启动项目、关闭不必要的服务、关闭缩略

图缓存、设置合适的虚拟内存等方法解决。

(3) 监视服务器的可靠性和性能的工作，则可以使用 Windows Server 2008 服务器提供的可靠性和性能监视器来完成。

3.2 Server Core

微软公司为了使硬件发挥最大的效能，推出了 Windows Server 2008 Server Core，即 Windows Server 2008 服务器核心。Server Core 以安全性、稳定性为第一要务，只提供 Windows 核心基础服务，没有图形界面，只能通过命令提示符窗口以命令行方式运行。由于运行的组件少，从而减少了对其他服务和管理工具的攻击范围与风险。

3.2.1 Windows Server Core 概述

操作系统不稳定、漏洞多，一向是 Windows 系统的缺点。但微软推出的 Windows Server 2008 Server Core，使得这种情况大为改观。

1. Server Core 的优点

Windows Server 2008 Server Core 主要具备以下优点。

(1) 服务器的稳定性更高。由于 Server Core 安装的功能较少，并且只用来运行很少的服务和应用，因此，系统漏洞和占用的资源也更少，与运行了更多功能的服务器相比，极大地提高了服务器的稳定性和性能。

(2) 减少软件维护量。由于 Server Core 只安装最基本的功能，因此，所需要管理的软件也就更少，从而提高了管理性，降低了软件维护量，例如，需要更新和安装补丁的软件更少了。

(3) 降低被攻击风险。服务器只安装有限的服务和应用，因此，暴露在网络中的攻击点也就很有限，从而使攻击者的攻击面更少，很大程度上降低了被攻击的可能性。

(4) 空间占有率更少。Server Core 没有安装不必要的驱动、应用和图形界面，因此，安装后只占用 1GB 左右的磁盘空间，是正常 Windows Server 2008 的 1/6，并且安装完成之后，由于运行的程序更少，对服务器的资源占有率也大大降低。同时，只有需要角色的文件才会被安装，对于 IE、.NET 框架等则不会安装。

提示： Server Core 中的命令不区分大小写。

2. Server Core 的缺点

Server Core 最大的缺点就是使用起来不方便。由于所有的管理全部使用命令行完成，因此，对于已经熟悉 Windows 图形化界面的网络管理员来说，难度比较大，不仅需要熟悉命令行模式下的管理模式，同时更要记住复杂的命令。不过，如今已经有了专门用于 Server Core 系统的图形化软件，可以方便用户的使用。

3. Windows Server Core 的安装

Windows Server Core 的出现取代了 Windows Server 2008 系统的额外组件，核心操作系统比普通的 Windows Server 2008 完全安装更简单。因为安装的组件少，所以攻击面小，管理和维护的费用也比较少。Server Core 只允许操作系统必需的重要组件，即支持 Windows Server Core 安装上可用的各种角色和功能。许多没有添加值的旧版组件和客户端组件都不会在 Server Core 中出现。

Server Core 安装，这种优化安装主要是基于特定的角色，例如域控制器或文件服务器，如下所示。

（1）Server Core 的攻击面较小，因为安装的组件少，稳定性较高。

（2）由于安装的组件少，因此 Server Core 安装比普通的完全安装应用的补丁程序少。经常出现与 Internet Explorer 稳定性相关的紧急修补程序，若没有安装 Internet Explorer，就不运行应用修补程序。如果在 Windows 2000 系统中 Server Core 安装可用，要求的修补程序会比普通的完全安装少 60%；如果是在 Windows Server 2003 系统中 Server Core 安装可用，要求的修补程序会比完全安装少 40%。Windows Server 2008 下载的服务包只在系统上安装的组件上应用。Server Core 不要求进行任何操作或特殊的 Windows 更新站点。

（3）没有安装额外的组件，所以可以把注意力放在技术方面，不用担心常规的 Windows 知识。

（4）运行的组件少，安装使用的系统资源较少，可靠性有所提升，出现故障的频率也有所减少。

（5）占用更少的磁盘空间。典型的核心安装使用 1GB 磁盘空间进行安装，其他磁盘空间用于实际操作。Windows Server 2008 安装只要求 512MB 的 RAM。

Server Core 安装选项可用的平台包括 Windows Server 2008 的标准版、企业版和数据中心版，而且均包括 x86 和 x64 不同平台。

Server Core 是最简单的 Windows 安装，所以并不是所有 Windows Server 组件都可以运行，例如，Server Core 中.NET Framework 未安装，所以共通语言执行平台（Common Language Runtime，CLR）和管理代码都无法运行，也无法运行 PowerShell。Server Core 不安装的组件如下所示。

（1）没有基于 Explorer 的 Shell，所以没有“开始”按钮、任务栏通知区域（系统任务栏）和任务栏。没有壁纸和桌面保护程序（默认的桌面保护程序显示 Windows Server 2008 标识），没有 Aero Glass 画面。Explorer 本身不可用，所以没有资源管理器。没有系统任务栏，也就没有通知，没有密码提示。

（2）无 Explorer 意味着没有 Internet Explorer，没有搜索、运行和帮助。但可以使用记事本。

（3）无.NET Framework。

（4）无 Microsoft 管理控制台（Microsoft Management Console，MMC），意味着没有管理单元。

（5）只有两个控制面板应用程序。

Server Core 没有图形界面、管理工具、浏览器、控制面板应用程序，Server Core 拥有一个 Shell，那就是命令提示符。所有的 MMC 管理单元都可以连接到远程计算机，帮助管理无图形界面的 Server Core 安装。

之前只有 Active Directory 域服务器（域控制器），DNS、DHCP 和文件服务器可用。现在拥有更多的可用角色。Windows Server 中的角色是 Windows Server 2008 中非常重要的组件，功能虽然比角色的重要性稍差，但可以帮助更好地实现角色。表 3-1 列出了 Windows Server Core 中可用的角色和功能。需要注意的是，这些角色和功能之前没有任何关系，将其放在一起只是为了节省空间。

表 3-1 Windows Server Core 角色和功能

Server Core 角色	Server Core 功能
Active Directory 域服务(ADDS)	BitLocker 驱动程序加密(和远程管理工具)
Active Directory 轻型目录服务(通常称为 ADAM)	故障转移群集
DHCP 服务器	多路径 I/O
DNS 服务器	NAP 客户端
文件服务	Qos(Qwave)
Internet 信息服务(IIS)	可移动存储管理
打印服务	简单网络管理协议(SNMP)服务
流媒体服务	基于 UNIX 应用程序的子系统
Windows Server 虚拟化(Hyper-V)	Telnet 客户端 Windows 进程激活服务 Windows Server 备份 WINS 服务器

3.2.2 安装 Windows Server Core

Server Core 并没有独立的安装进程,因为 Server Core 安装和 Windows Server 2008 的普通完全安装基本相同。安装位置被放置在服务器和服务器启动中,只需输入产品密钥来识别 Windows Server 2008 的不同版本。Server Core 安装和完全安装的差别在于,输入产品密钥后,需要在图 3-1 所示的"选择要安装的操作系统"对话框内选择 Windows Server 2008 的安装类型(完全安装或服务器核心安装)。

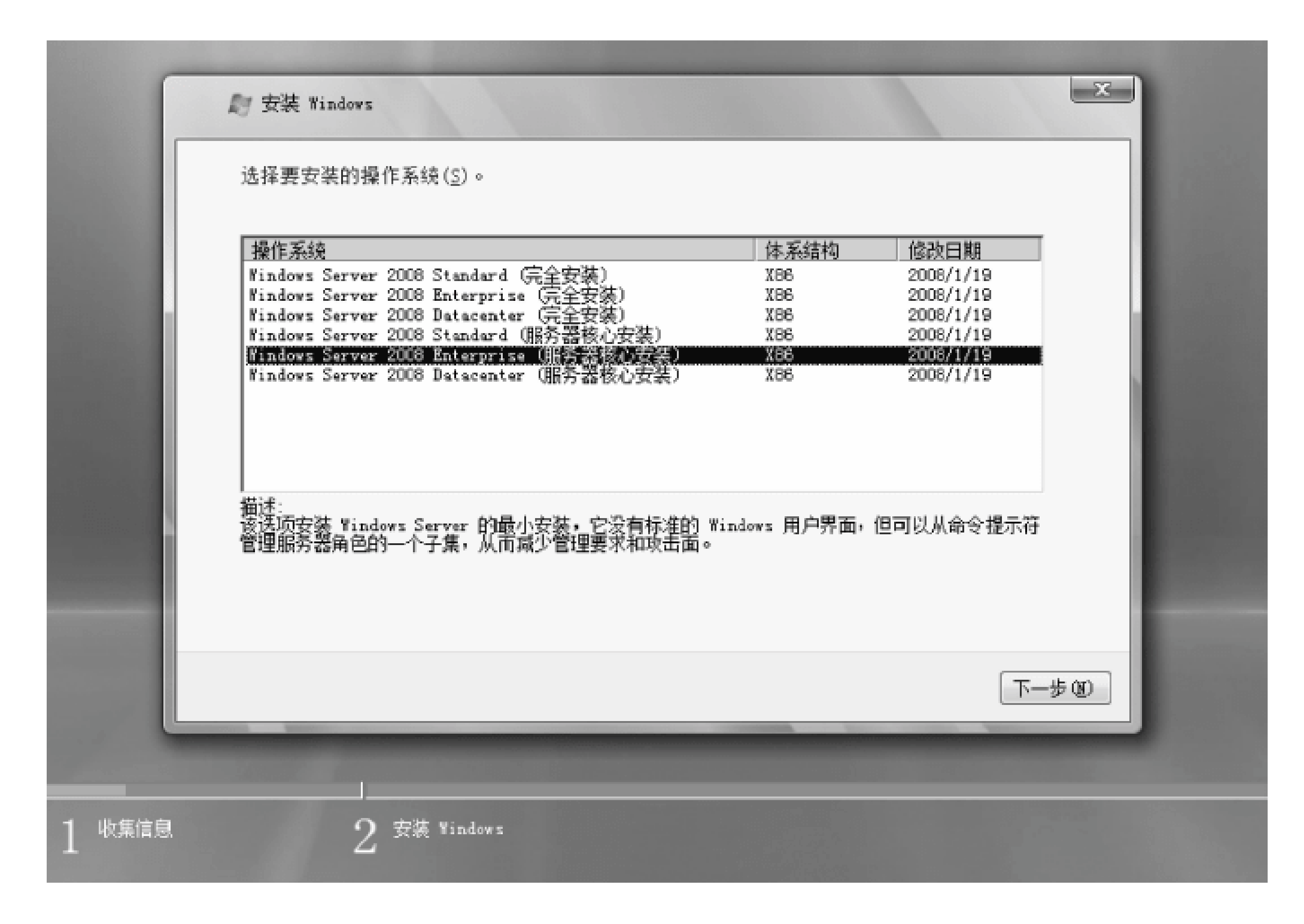


图 3-1 "选择要安装的操作系统"对话框

然后根据提示安装完成即可,安装完成后,显示"按 CTRL+ALT+DELETE 登录"界面,界面的底部显示 Windows Server 登录。如果按键的顺序正确,提示输入登录凭据。现在可以以管理员账户的身份登录,密码空白。按 Ctrl+Alt+Delete 键,显示图 3-2 所示的选择用户界面。



图 3-2　选择用户界面

单击“其他用户”按钮，显示图 3-3 所示的登录窗口，提示需要输入用户名和密码登录。

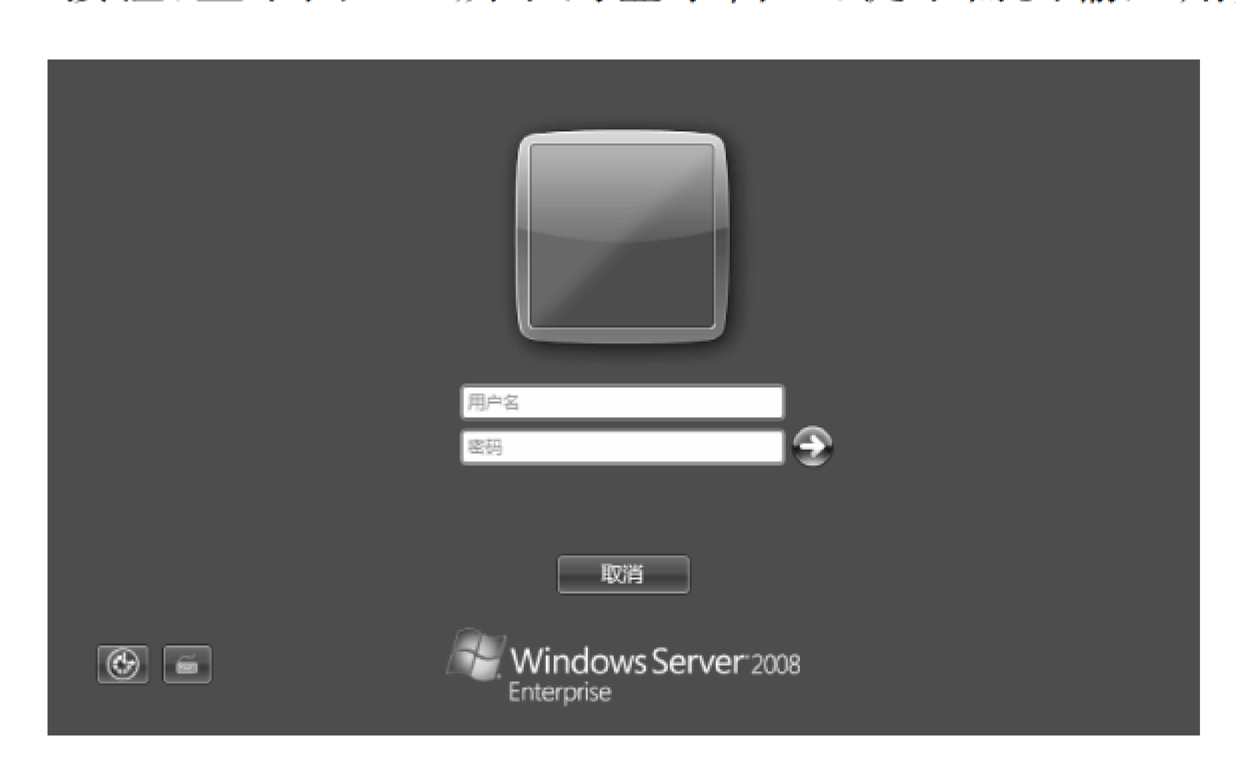


图 3-3　登录窗口

在“用户名”文本框中输入管理员用户名 administrator，不需输入密码，按 Enter 键确认，提示需要更改密码。在 Server Core 刚刚安装完成时，只有一个管理员账户 administrator，并且必须设置一个强密码才能登录。单击“确定”按钮，显示图 3-4 所示的窗口，提示重新设置密码。在“新密码”和“确认密码”文本框中输入一个新密码，以后登录系统时，都需要使用该密码登录，而“密码”文本框中不需输入内容。



图 3-4　设置新密码

按 Enter 键确认，显示图 3-5 所示的界面，提示密码已更改。应用本地策略，预备桌面。

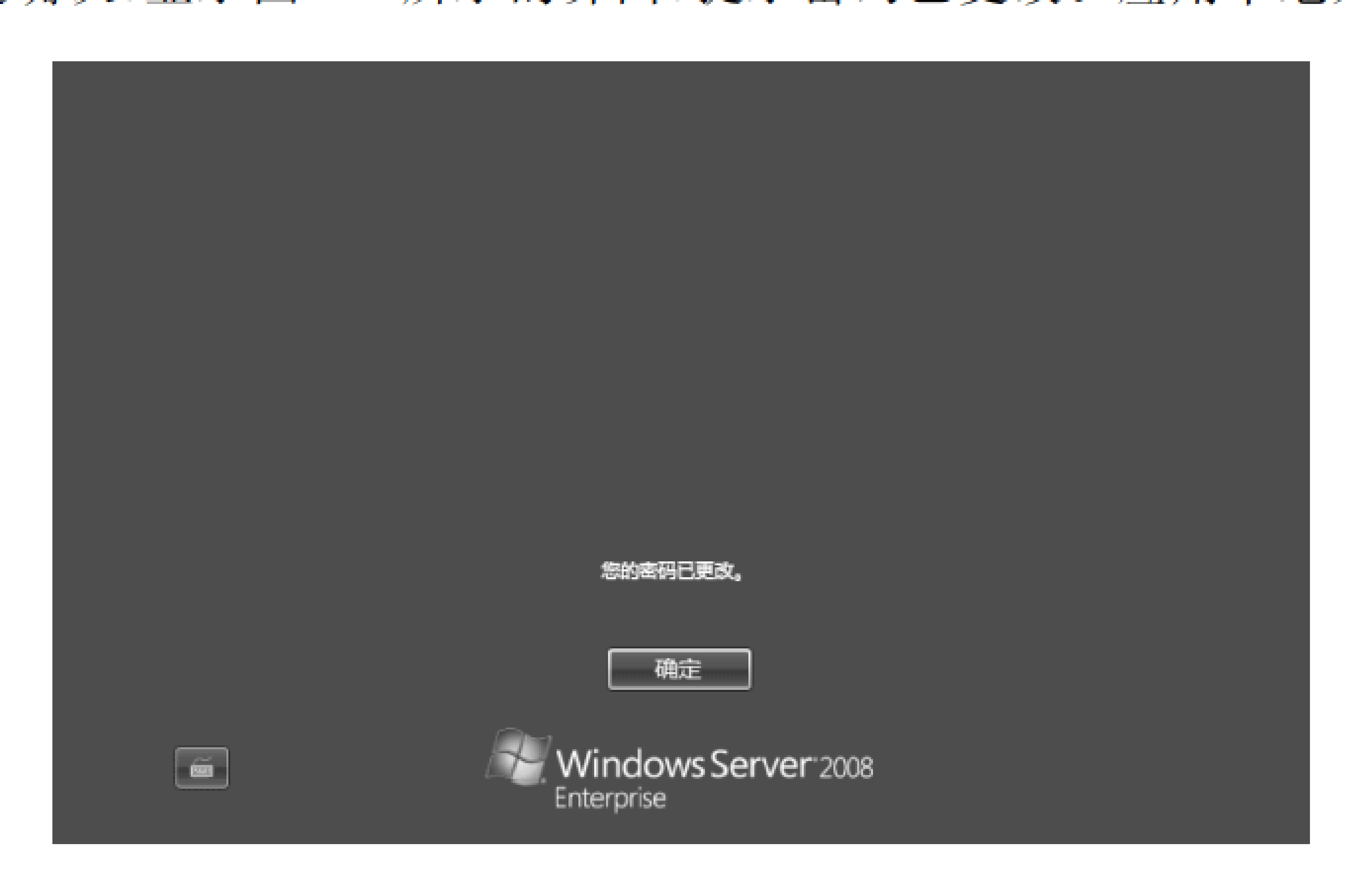


图 3-5　密码已更改

单击"确定"按钮，即可登录到 Windows Server 2008 Server Core，加载 Server Core 桌面。成功登录系统后，只有一个命令提示符窗口，没有其他菜单及文件夹窗口，如图 3-6 所示。

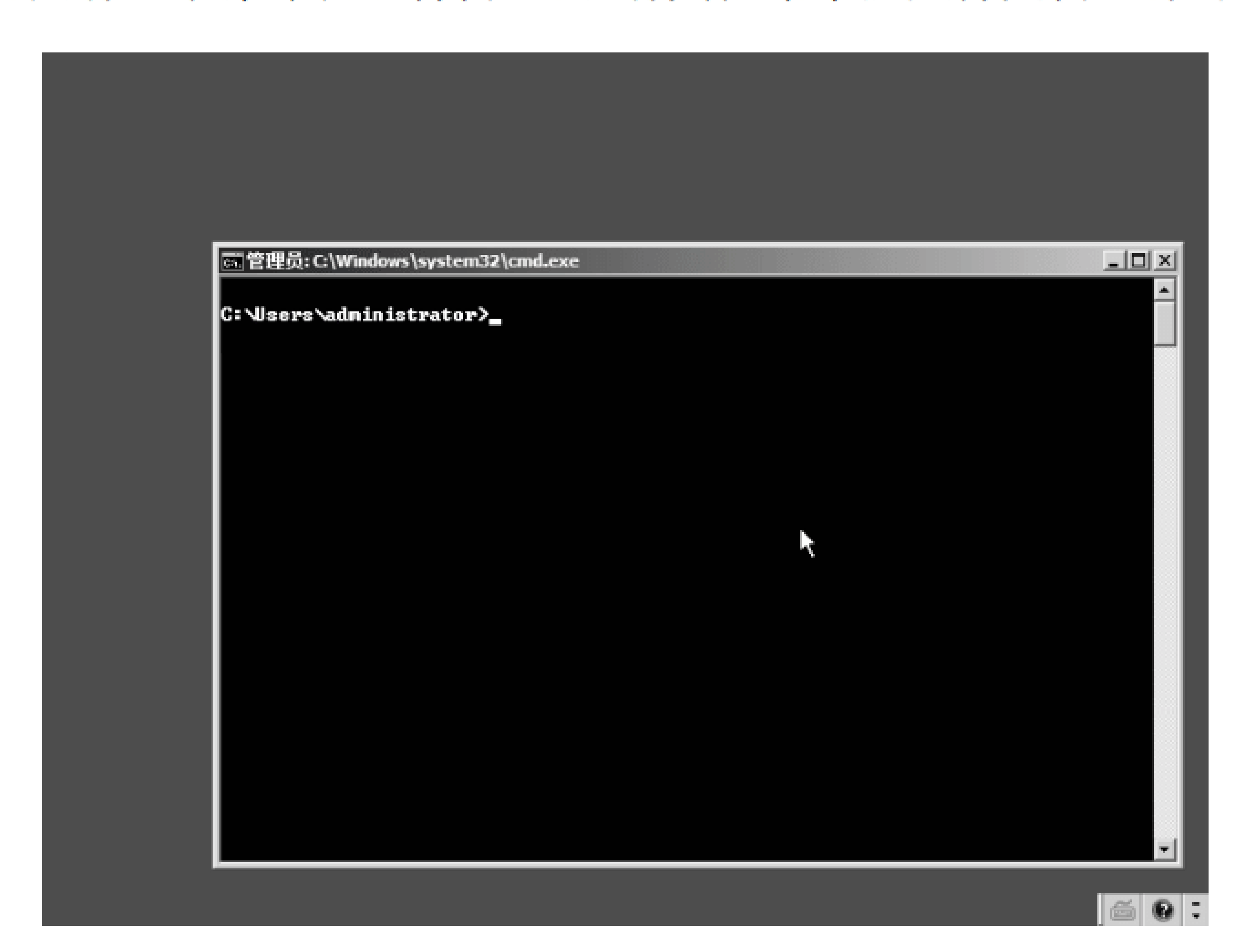


图 3-6　命令提示符

至此，Windows Server 2008 Server Core 安装完成，所有的服务配置均可在该命令提示符窗口中完成。

需要注意的是，不可以从 Windows Server 2003 升级至 Server Core，只支持新安装的 Server Core。也不可以从 Server Core 升级至完整的 Windows Server 2008 产品，或者从 Windows Server 2008 降级至 Server Core。若需要在这两个版本之间进行切换，需要执行全新的安装。

3.2.3　配置 Server Core

安装 Server Core 后，要对其进行配置。由于没有普通的图形界面，因此不可以使用初

始配置任务(Initial Configuration Tasks,ICT)界面配置 Windows Server 2008 服务器,需要使用如下两个方法实现。

(1) 使用命令行工具手动配置服务器。

(2) 在实际安装过程中使用应答文件自动配置。

一般情况下可以使用 GUI 界面完成这些配置任务,例如,使用网络和共享中心配置 IP 设置、使用 Windows 更新配置修补程序等。但这些界面在 Server Core 安装中都不可用。所以需要使用命令行和 Server Core 特定的命令完成这些配置。其中大部分标准命令也适用于普通安装。

1. 设置管理员密码

Server Core 安装与标准安装的系统在密码安全方面基本相同,所以要更改登录账户的密码,可以直接按 Ctrl+Alt+Delete 键。在菜单中选择“更改密码”命令,在“更改密码”对话框进行修改即可。

在任何其他 Windows 操作系统上运行 net user 命令并传送用户名和新密码或者传送新密码提示的星号字符(*),也可以更改密码,如图 3-7 所示。要更改域账户密码,还需要添加/domain 参数。



图 3-7　使用命令行更改密码

2. 设置服务器名称

默认情况下,在安装 Windows Server 2008 时都不需要设置计算机名,系统会随机生成一个计算机名,Server Core 也是如此。但在实际应用中,随机生成的名字没有实际意义,也不便于记忆,因此,在安装完操作系统后需要更改服务器名。

利用 hostname 命令可以查看当前计算机名,而重命名则需要利用 netdom 命令来实现。

(1) 在命令提示符中输入如下命令。

```
hostname
```

按 Enter 键,可以查看当前的计算机名,如图 3-8 所示。



图 3-8　显示当前计算机名

(2) 现在即可利用 netdom 命令来更改计算机名,格式如下。

```
netdom renamecomputer 旧服务器名称 /Newname:新服务器名称
```

例如:

```
netdom renamecomputer WIN-I2GUSJXLNZJ /newname:core
```

按 Enter 键运行,提示重命名计算机可能导致某些服务不能正确运行,并询问是否要继续。

(3) 输入 y,按 Enter 键,命令成功完成,如图 3-9 所示。同时,提示需要重新启动系统,新计算机名才能生效。

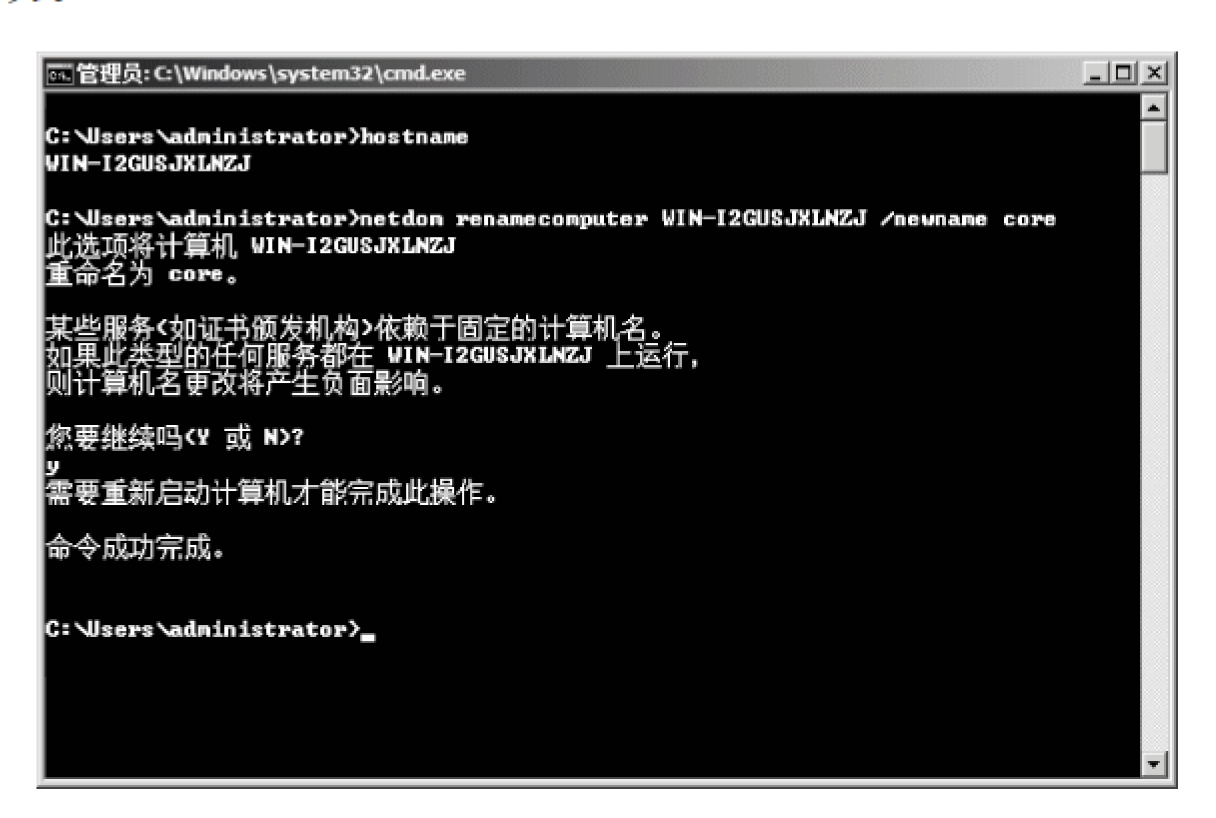


图 3-9 重命名完成

(4) 运行 shutdown 命令重新启动计算机。为了加快关机速度,可设置关机延时为两秒。在命令提示符中输入如下命令。

```
shutdown /r /t 2
```

按 Enter 键,重新启动计算机并登录,即可应用新的计算机名,重命名工作完成。

3. 设置 IP 地址

Server Core 安装完成后,默认以 DHCP 模式分配 IP 地址。由于服务器通常使用静态 IP 地址,因此,需要在安装完成后为系统设置静态 IP 地址。

设置 IP 地址可使用 netsh 命令来完成。这里,将设置服务器的 IP 地址为 192.168.1.9,子网掩码为 255.255.255.0,网关为 192.168.1.254,DNS 服务器为 211.82.216.5。

(1) 在命令提示符中输入如下命令。

```
netsh interface ipv4 show interfaces
```

该命令的作用是显示使用 IPv4 协议的网络连接。按 Enter 键,命令成功执行,显示了服务器中可用的网络连接,本地连接的 ID 为 2。

(2) 下面开始设置静态 IP 地址。在命令提示符中输入如下命令。

```
netsh interface ipv4 set address name="2" source=static address="192.168.1.9" mask="255.255.
255.0" gateway="192.168.1.254"
```

按 Enter 键,命令成功执行,服务器的 IP 设置成功。在该命令中,set address name="2" 表示所设置的本地连接的 ID,source=static 表示设置静态 IP 地址,address 表示 IP 地址,

mask 表示子网掩码，gateway 表示网关。

提示：也可以使用简写的命令格式来添加 IP 地址。

```
netsh interface ipv4 set address "本地连接" static 192.168.1.9 255.255.255.0 192.168.1.254
```

(3) 然后，再设置 DNS 服务器地址。在命令行提示符中输入如下命令。

```
netsh interface ipv4 add dnsserver name="2" address="211.82.216.5" index=1
```

按 Enter 键，命令成功执行，如图 3-10 所示，即可将服务器的首选 DNS 服务器设置为 202.99.160.68。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\administrator>netsh interface ipv4 show interfaces

Idx  Met   MTU   状态          名称
---  ---  -----  -----------  -------------------
  2   10   1500  connected    本地连接
  1   50 4294967295  connected     Loopback Pseudo-Interface 1

C:\Users\administrator>netsh interface ipv4 set address name="2" source=static a
ddress="192.168.100.40" mask="255.255.255.192" gateway="192.168.100.62"

C:\Users\administrator>netsh interface ipv4 add dnsserver name="2" address="192.
168.100.5" index=1

C:\Users\administrator>
```

图 3-10 设置 IP 地址信息

设置完成以后，运行 ipconfig /all 命令可以查看当前详细的 IP 地址信息，如图 3-11 所示。

```
管理员: C:\Windows\system32\cmd.exe
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel 21140-Based PCI Fast Ethernet Adapt
er (Emulated)
   物理地址. . . . . . . . . . . . . : 00-03-FF-0C-40-5D
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::f90f:11b5:b73e:4318%2(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.100.40(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.192
   默认网关. . . . . . . . . . . . . : 192.168.100.62
   DNS 服务器  . . . . . . . . . . . : 192.168.100.5
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

隧道适配器 本地连接*:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : isatap.{E4C362EF-64EA-44BB-99BB-B2D220B48
15D}
   物理地址. . . . . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是

隧道适配器 本地连接* 3:
```

图 3-11 查看 IP 地址

4. 设置时区

使用 date 和 time 命令行可以轻松设置日期与时间。但使用命令行设置时区有一点难度。时区中包含注册表区域，但没有必要使用注册表。Server Core 中控制面板不可用，但

有两个程序可用，其中一个是日期和时间控制面板程序。运行下列命令启动日期和时间控制面板程序。

```
control timedate.cpl
```

加载程序后，如图 3-12 所示，执行普通的日期/时间和时区配置即可。

注意： 域环境内时间必须同步，但还是要设置时区。



图 3-12 配置日期/时间和时区

5. 加入域

与图形界面的 Windows Server 2008 一样，Server Core 也可以加入域，使用域中的资源并为网络提供服务。不过，在加入域之前，必须先将 Server Core 的 DNS 服务器地址设置为域控制器的 IP 地址，并且应利用 Ping 命令测试 Server Core 与域控制器的连通性。

将 Server Core 加入域需使用 netdom join 命令，命令格式如下。

```
netdom join machine /Domain:domain [/UserD:user] [/PasswordD:[password | *]] [/REBoot[:Time in seconds]]
```

该命令中参数的含义如下。

(1) machine：要加入域的成员计算机名。

(2) /Domain:domain：指定要加入域的域名。

(3) /UserD:user：有权限加入域的域用户。

(4) /PasswordD:[password | *]：输入域用户账户的密码。

(5) /REBoot[:Time in seconds]：指定计算机在加入域后，多长时间关闭并自动重新启动。默认值是 30 秒。

这里，使用域管理员账户 Administrator 将 Server Core 加入域。具体操作步骤如下。

(1) 设置 Server Core 的 DNS 服务器。首先将域控制器的 IP 地址添加到 Server Core 的 DNS 服务器地址中。在命令提示符下输入如下命令。

```
netsh interface ipv4 add dnsserver name="2" address="192.168.100.5"
```

按 Enter 键，DNS 服务器地址添加完成。

（2）将 Server Core 加入域。为了安全起见，不在屏幕上显示密码，因此使用参数：/PasswordD：* 。在命令提示符下输入如下命令。

```
netdom join core /Domain:coolpen.net /UserD:administrator /PasswordD: *
```

按 Enter 键，命令成功执行，提示输入域用户的密码，如图 3-13 所示。

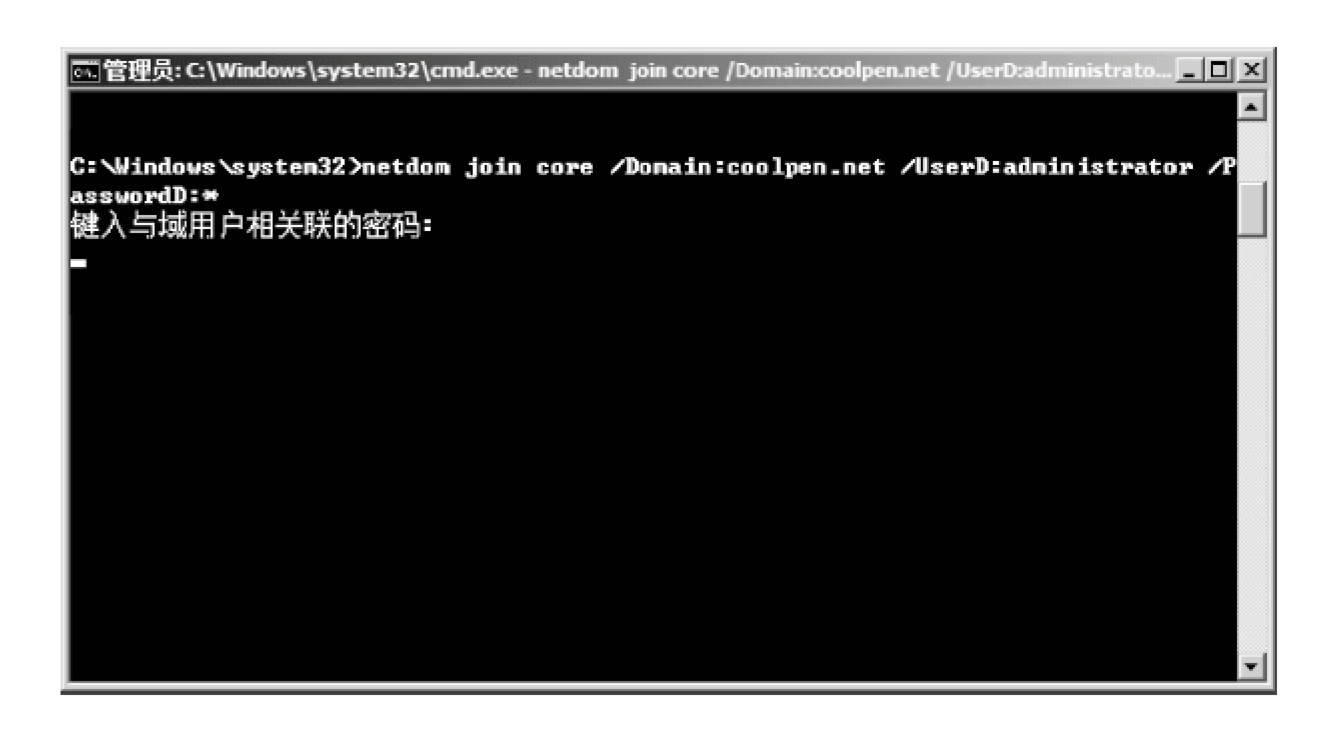


图 3-13　输入域用户密码

提示：如果在运行命令时直接输入了密码，将不会出现该提示。

（3）在光标处输入域用户的密码即可。需要注意的是，当输入密码时，并不会显示密码的字符，从而防止密码泄露。完成后直接按 Enter 键，稍候即可加入域，并提示需要重新启动计算机才能完成此操作，如图 3-14 所示。

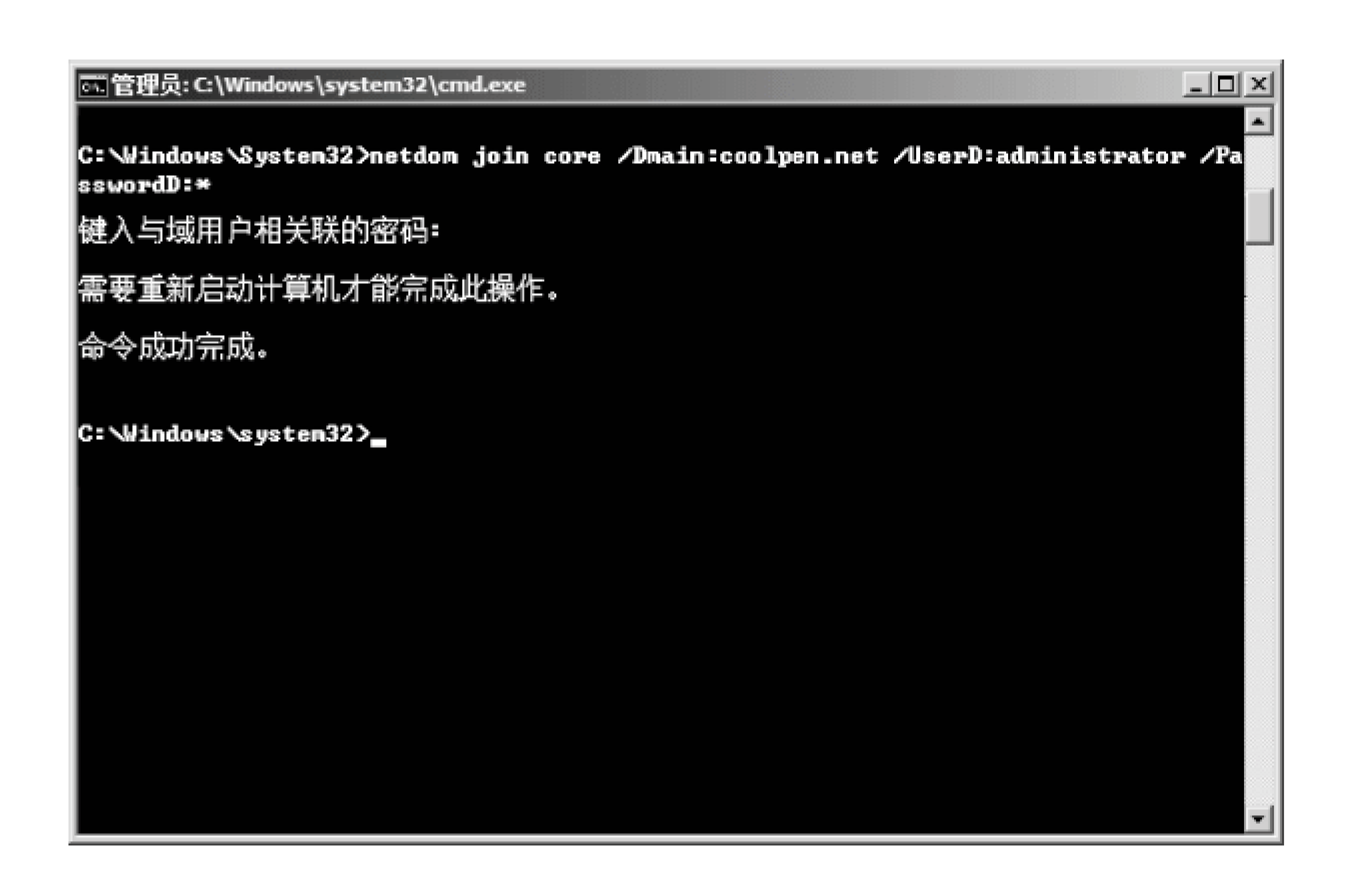


图 3-14　加入域成功

（4）运行 shutdown 命令重新启动服务器，即可登录到域了。在登录界面单击“切换用户”按钮，再单击“其他用户”按钮，显示图 3-15 所示的界面。在“用户名”文本框中输入域用户账户；格式为：域名/域用户名；在“密码”文本框中输入域用户的密码。

（5）按 Enter 键，即可登录到域，如图 3-16 所示。

提示：如果要退出域，可使用 netdom remove 命令。



图 3-15 使用域用户登录



图 3-16 已登录到域

6. 激活服务器

Server Core 包含 Slmgr.vbs 脚本。使用该脚本和-ato 参数可以执行操作系统的自动激活。Slmgr.vbs 并不是 Server Core 的一个功能,而是在 Windows Vista 和完全 Windows Server 2008 部署中,是 Windows Vista 和 Windows Server 2008 产品的主要许可证管理器。

Server Core 没有任务栏和系统通知区域,所以无法接受激活服务器的任何提示,需要安装 Server Core 之后立即激活服务器。

激活服务器之前,首先使用-xpr 参数查看 30 天宽限期的剩余时间。

```
C:\Users\Administrator>cscript slmgr.vbs -xpr
初始宽限期于 2009/9/20 11:06:17 过期
```

使用-dli 参数和-dlv 参数可以获取更多的详细信息。

```
C:\Users\Administrator>cscript slmgr.vbs -dli
名称: Windows Server(R), ServerEnterpriseCore edition
```

```
描述: Windows Operating System - Windows Server(R), VOLUME_KMSCLIENT channel
部分产品密钥: X4Q6V
许可证状态: 初始宽限期
剩余时间: 86160 分钟(59 天)
```

如果有普通的许可证密钥或者多个激活密钥(Multiple Activation Key,MAK),可以直接进行激活。如果拥有本地密钥管理服务(Key Management Service,KMS),则通过-skms <KMS server>参数使用 KMS 进行激活。若需要清除已配置的 KMS 服务器,可以使用-ckms 参数;若正在使用企业许可证密钥,可以使用-ipk <key>参数。

要激活服务器可以使用-ato 参数。重新运行显示的许可证信息,查看状态,显示无剩余时间。

```
C:\Users\Administrator>cscript slmgr.vbs -ato
正在激活 Windows Server(R), ServerEnterpriseCore edition (c1af4d90-d1bc-44ca-85d
4-003ba33db3b9) ...
产品成功激活.
C:\Users\Administrator>cscript slmgr.vbs -dli
名称: Windows Server(R), ServerEnterpriseCore edition
描述: Windows Operating System - Windows Server(R), VOLUME_KMSCLIENT channel
部分产品密钥: X4Q6V
许可证状态: 初始宽限期
```

7. 启用自动更新

为了保障操作系统的安全,应及时从微软网站下载更新程序,以修补漏洞、增加系统性能。因此,自动更新是操作系统必不可少的功能。在 Server Core 中,同样也需要启用自动更新功能。

登录到 Server Core 系统以后,在命令提示符中输入如下命令。

```
cscript c:\windows\system32\scregedit.wsf /au 4
```

按 Enter 键运行,提示"已更新注册表",已经启用了自动更新功能,如图 3-17 所示。其中,数字 4 表示启用自动更新,如果禁用自动更新则使用数字 1。



图 3-17　启用自动更新

使用/v 参数则可查看当前的配置状态。在命令提示符中输入如下命令。

```
cscript c:\windows\system32\scregedit.wsf /au /v
```

按 Enter 键，显示如图 3-18 所示，可以查看注册设置。这里显示数值为 4，表示已启用自动更新。



图 3-18 查看自动更新状态

8. 启用远程桌面

Server Core 同样支持远程桌面管理功能，可以在网络中的远程计算机上利用远程桌面进行管理。不过，需要先在 Server Core 服务器上更改注册表设置，同时在防火墙启用远程桌面端口后，客户端计算机才能够连接服务器。

（1）以管理员身份登录到 Server Core 系统，在命令提示符中输入如下命令。

```
cd c:\windows\system32
```

按 Enter 键运行，进入系统目录。

（2）在命令行提示符中输入如下命令。

```
cscript scregedit.wsf /ar 0
```

按 Enter 键运行，即可更新注册表，启用远程管理功能。

（3）在命令行提示符中输入如下命令。

```
slmgr.vbs -ato
```

按 Enter 键，激活服务器，如图 3-19 所示。

此时，为 Server Core 服务器启用了远程桌面功能，即可在客户端计算机上远程连接并进行管理了。

9. 服务器关机

服务器在配置网络服务或更改系统配置时，经常会要求重新启动。但由于 Windows Server 2008 Server Core 中没有图形界面，因此，无法像普通 Windows 一样通过“开始”菜单来关机、注销和重新启动。不过，可以使用 shutdown 命令来实现这些操作。该命令在图形界面的 Windows Server 2008 中同样适用。



图 3-19　启用远程管理功能

例如，现在要关闭计算机，可在命令提示符中输入如下命令。

shutdown /s

按 Enter 键运行，显示图 3-20 所示的“您将要被注销”对话框，提示“Windows 将在一分钟内关闭”。一分钟之后，系统就会自动关闭。

注意：如果此时单击“关闭”按钮，虽然可关闭该对话框，但关机计划不会中止，仍在后台运行。

如果想要让系统自动重新启动，并且设置延时为 10min(10min=600s)，可在命令提示符中输入如下命令。

shutdown /r /t 600

按 Enter 键，显示图 3-21 所示的“您将要被注销”对话框，提示“Windows 将在 10 分钟内关闭”。当达到 10 分钟的设置时间后，系统就会自动关机并重新启动。

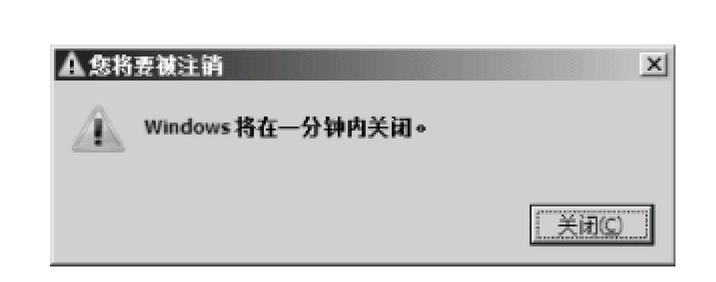


图 3-20　“您将要被注销”对话框

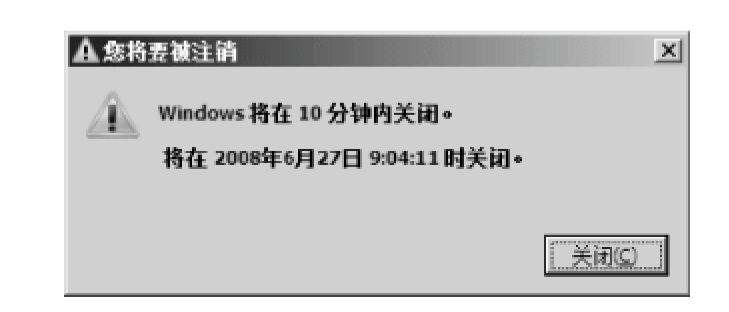


图 3-21　10 分钟后关闭 Windows

提示：如果所设置的延时时间少于一分钟，在提示框中就会显示为“Windows 将在一分钟内关闭”。

shutdown 命令的语法格式如下。

shutdown [/i | /l | /s | /r | /g | /a | /p | /h | /e] [/f] [/m \\computer][/t xxx][/d [p|u:]xx:yy [/c "comment"]]

shutdown 命令的常用参数如下。

(1) /?：与不输入任何参数一样，显示帮助信息。

(2) /：立即注销当前账户。

(3) /s：关闭计算机。

(4) /r：关闭并重新启动计算机。

(5) /g：关闭并重新启动计算机。但系统重新启动后，重新启动所有注册的应用程序。

(6) /t xxx：设置关机延时时间为 xxx 秒，有效范围为 0～600，默认为 30。默认已设置 /f 参数。

(7) /a：中止系统关闭，但只能在超时期间内使用。

(8) /c "comment"：注释重启动或关闭的原因。最多允许 512 个字符。

(9) /f：强制关闭正在运行的应用程序，且不出现警告。使用 /t xxx 默认使用 /f。

注意：在使用/s、/r 等命令关闭或重新启动系统时，如果不加/t xxx 参数，则默认延时时间为一分钟。

10. 添加角色和功能

与普通 Windows Server 2008 相同，Windows Server Core 在安装完成后，安装的角色和功能非常少。此时，可根据需要安装所需的角色或功能。在 Windows Server Core 中，不能访问普通的服务器管理器界面添加角色和服务，所有功能（ADDS 除外）都是通过 Ocsetup 命令添加的。需要注意的是，该命令区分大小写，是所有 Windows Server 2008 安装的一个组成部分。安装 Active Directory 时，通过 dcpromo 命令安装二进制文件，通过无人参与应答文件安装配置项。不可以使用 DCPROMO GUI，只能使用无人参与应答文件或命令行参数。有关无人参与 Active Directory 安装的更多信息，参考其他相关资料，这里就不再赘述。

卸载角色和功能使用的命令与添加角色和功能的命令相同，只不过要在末尾添加/uninstall 参数。唯一的例外是 ADDS，卸载 ADDS 要使用 DCPROMO。

表 3-2 和表 3-3 分别列出了组件的名称以及这些组件在功能和角色中对应的名称。运行 oclist 命令可以获取完整列表，该命令是 Server Core 特定的命令。

表 3-2 服务器角色和 Ocsetup 名称

服务器角色	Ocsetup 名称
Active Directory 轻型目录服务(ADAM)	DirectoryServices-ADAM-ServerCore
DHCP	DHCPServerCore
DNS	DNS-Server-Core-Role
分布式文件系统服务	DFSN-Server
分布式文件系统复制(DFSR)	DFSR-Infrastructure-ServerEdition
文件服务	File-Server-Core-Role
文件复制服务(FRS)	FRS-Infrastructure
IIS(无 ASP. NET)	IIS-WebServerRole(加上可视的组件)
网络文件系统(NFS)	ServerForNFS-Base
媒体服务器	MediaServer
Hyper-V	Microsoft-Hyper-V

表 3-3　服务器功能和 Ocsetup 名称

服务器功能	Ocsetup 名称
备份	WindowsServerBackup
BitLocker 驱动程序加密	BitLocker
BitLocker 远程管理工具	BitLocker-RemoteAdminTool
故障转移群集	FailoverCluster-Core
多路径 IO	Microsoft-Windows-MultipathIO
NFS 客户端	ClientForNFS-Base
网络负载平衡	NetworkLoadBalancingHeadlessServer
服务质量	QWAVE
可移动存储管理	Microsoft-Windows-RemovableStorageManagementCore
SNMP	SNMP-SC
基于 UNIX 应用程序的子系统	SUACore
Telnet 客户端	TelnetClient
Windows 激活服务(WAS)	WAS-WindowsActivationService
WINS	WINS-SC

默认情况下，若运行 Ocsetup 命令时有工具包要安装，则在后台安装时立即返回命令提示符，而且不显示完成安装时间。为了解决这一问题，需要在 start/w 通知执行命令并在执行完成后运行 Ocsetup 命令。下面以安装 DHCP 服务器角色为例进行说明，在命令提示符下输入如下命令。

```
start /w Ocsetup DHCPServerCore
```

按 Enter 键，即可成功安装 DHCP 服务。需要注意的是，在安装过程中不会显示任何提示。安装完成以后，运行 oclist 命令，可以看到“已安装：DHCPServerCore”提示，表示 DHCP 服务器角色已安装，如图 3-22 所示。

提示：如果要卸载 DHCP 服务，可运行命令：start /w Ocsetup DHCPServerCore /uninstall，并且会显示图 3-23 所示的提示框，提示需要重新启动系统才能生效。



图 3-22　已安装 DHCPServerCore

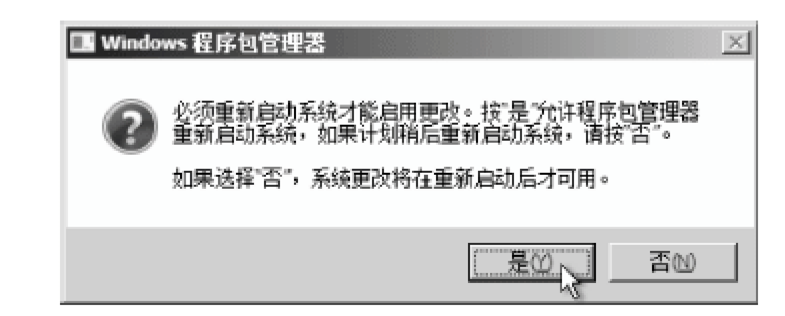


图 3-23　卸载 DHCP 服务

11. 安装应用程序

在 Windows Server 2008 中，Server Core 只运行开机即用功能，即所支持的服务器角色和功能，而不是额外的应用程序。

Server Core 不支持主要产品，例如 Exchange、SharePoint、SQL 等。Server Core 添加了管理代码支持后，可能会运行额外应用程序。但 Server Core 对添加的应用程序具有很高的要求，否则 Server Core 安装和普通 Windows 安装就没有差别而言了。

Server Core 上可以安装并支持代理，例如备份代理、Microsoft 操作管理器(Microsoft Operations Manager，MOM)和系统管理服务器(System Management Server，SMS)代理等。这些代理可以通过远程管理控制台功能进行管理。也可以在 Server Core 上安装防病毒代理，并进行远程管理，例如，在 Server Core 上运行 ForeFront。Server Core 上还可以安装虚拟机条目。如果代理没有 Shell 或 GUI 依赖项，则不要求管理代码，这些代理就可以在 Server Core 上运行。

要安装额外软件，可以执行安装程序可执行文件或使用下列命令手动安装 MSI 文件。

```
msiexec /i <application>.msi
```

要检查已安装的应用程序，可以使用 wmic 命令和产品功能，如下所示。

```
C:\Windows\System32>wmic
wmic:root\cli>product
AssignmentType     Caption        Description
1                  VMware Tools   VMware Tools
```

卸载应用程序也可以使用 wmic 命令，检查应用程序的名称，然后调用卸载，如下所示。

```
C:\Windows\System32>wmic product get name /value
Name=VMware Tools
C:\Windows\System32>wmic product where name= "VMware Tools" call uninstall
```

3.3 系统性能优化

虽然 Windows Server 2008 系统安装或升级完成后即可正常使用，但是，此时的系统配置是为通用网络服务而设置的，难免有多余或者不足的组件。因此，系统管理员应当根据服务器所扮演角色的不同，进行一些必要的系统优化。

3.3.1 系统性能配置规划

目前，虽然服务器的硬件配置一般都比较高，但仍有可能不能满足需求。此时，则可以通过优化系统配置，提高系统性能，使服务器可以更好地为网络服务。

1. 禁用系统启动项目

某些应用程序在安装完成后会自动添加至系统启动组，以便在启动系统时自动运行。虽然方便了用户应用，但是这不仅延长了启动时间，还会在启动完成后自动占用系统资源。另外，对于服务器而言，只需启动必要的应用程序即可，因此建议将不必要的程序移除启动组。

2. 禁用不必要的服务

服务是服务器对网络提供服务的基础，默认情况下，Windows Server 2008 会按照微软所认为的用户服务要求启用服务，但这并不一定符合用户的具体网络要求，此时，则需要将不必要的服务关闭。

3. 关闭缩略图缓存

Windows XP/2003/2008 系统具有缩略图视图功能，用户可以在不打开图片文件的情况下看到缩小后的图片，并且可以将其保存在系统缓存中，再次浏览时可以直接从缓存中读取，加快了浏览速度，但同时也会占用大量的系统缓存。如果用户不希望系统进行缓存，则可以利用组策略关闭缩略图缓存的功能。

3.3.2 系统启动项目

依次选择"开始"→"运行"命令，在"打开"文本框中输入 msconfig 命令，单击"确定"按钮，即可启动系统配置实用程序。选择"启用"选项卡，如图 3-24 所示。通过选中或者取消选中指定"启用项目"前的复选框，即可控制其是否随系统启动而自动运行。

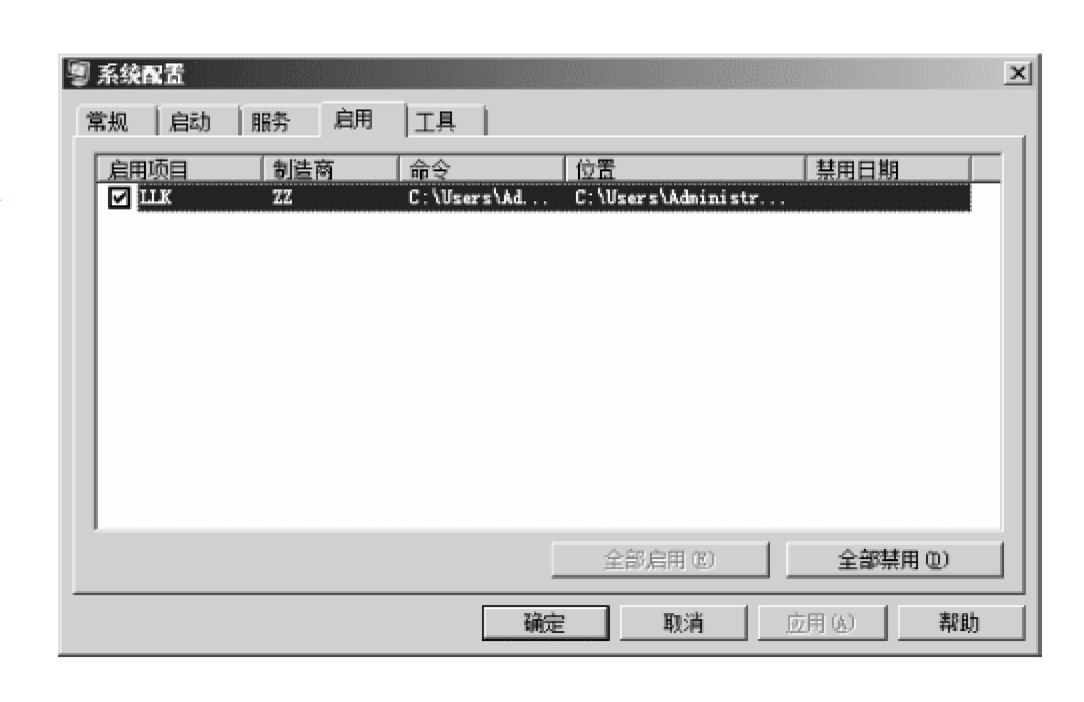


图 3-24 系统配置实用程序

3.3.3 关闭不必要服务

通常情况下，可以通过关闭相应服务的方法关闭非必要端口，例如，需要关闭 SNMP 陷阱服务，其操作步骤如下。

(1) 依次选择"控制面板"→"管理工具"→"服务"选项，系统显示"服务"控制台窗口，如图 3-25 所示。

(2) 在右侧的服务窗口中找到并双击 SNMP Trap 服务选项，系统显示图 3-26 所示的"SNMP Trap 的属性(本地计算机)"对话框。

(3) 如果服务已经启动，可以单击"停止"按钮停止该服务，然后在"启动类型"下拉列表框中选择"已禁用"选项。

(4) 单击"确定"按钮保存设置。

如果要开启该端口只要先在"启动类型"下拉列表框中选择"自动"选项，单击"确定"按钮，再打开该服务；在"服务状态"中单击"启动"按钮即可开放该端口；最后单击"确定"按钮即可。

3.3.4 关闭缩略图缓存

选择"开始"→"运行"命令，在打开的"运行"对话框中输入 gpedit.msc，然后单击"确定"按钮，打开"本地组策略编辑器"窗口。依次展开"用户配置"→"管理模板"→"Windows 组件"→"Windows 资源管理器"目录，双击"关闭缩略图的缓存"链接，打开其属性窗口，选中"已禁用"单选按钮，如图 3-27 所示。最后单击"确定"按钮，保存设置即可。需要注意的是，所修改的组策略并不会马上生效，需要等待系统自动更新组策略后才会生效。如果需要设置立即生效，可以在命令提示符中使用 gpupdate /force 命令，手动刷新组策略。



图 3-25 “服务”窗口

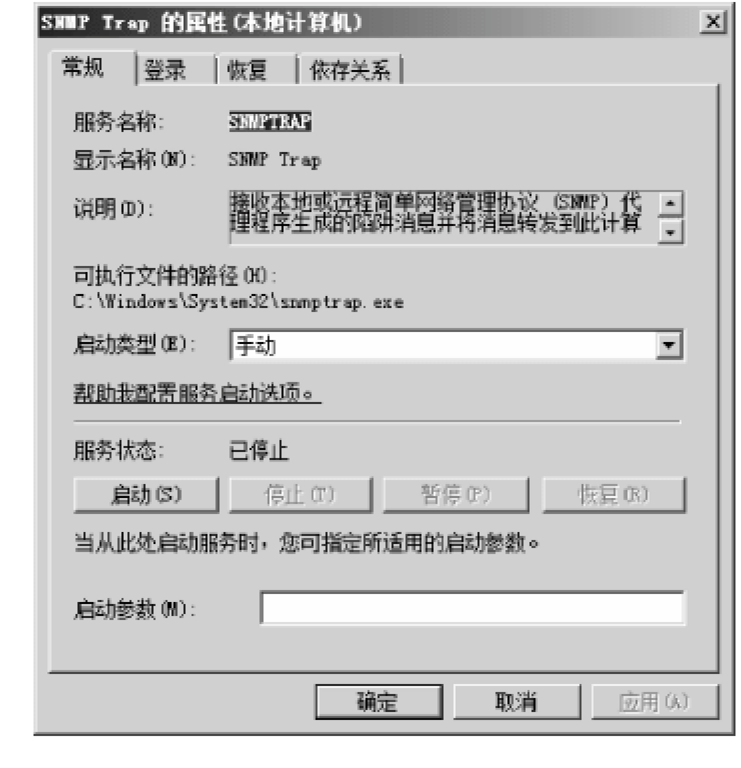


图 3-26 服务属性



图 3-27 关闭缩略图缓存

3.4 环境与系统变量的管理

内存是除 CPU 之外最重要的计算机组件之一。内存可用空间大小将直接影响到整个机器性能。随着操作系统和应用软件做得越来越大,对内存的要求也越来越高。但由于制作工艺的原因,物理内存的容量具有一定的局限性。因此为了解决内存容量不足的问题,微软推出了虚拟内存的概念,即使用硬盘的容量来实现内存的功能。

3.4.1 设置虚拟内存

物理内存通常被简称为内存,即实实在在存在的内存条。一般人们常说的 512MB 内存、1GB 内存都是指物理内存。而虚拟内存是在硬盘里划出一块空间,作为虚拟的“备用内存”,当物理内存不够时,即可调用虚拟内存。

虚拟内存是为了满足程序的运行要求，扩大可用"内存"空间而设置的。默认情况下，Windows Server 2008会自动管理所有驱动器的分页文件大小，但并不是所有情况都适合自动管理，因此，用户应根据实际需要修改虚拟内存的大小。

(1) 右击"计算机"图标，从快捷菜单中选择"属性"命令。在打开的"系统"窗口中单击"高级系统设置"按钮，打开"系统属性"对话框，然后选择图3-28所示的"高级"选项卡。

(2) 在"性能"选项区域中单击"设置"按钮，打开"性能选项"对话框，然后选择"高级"选项卡，如图3-29所示。

(3) 在"虚拟内存"选项区域中单击"更改"按钮，显示图3-30所示的"虚拟内存"对话框。取消选中"自动管理所有驱动器的分页文件大小"复选框，在"驱动器[卷标]"列表中，选择虚拟内存所在的硬盘分区(该分区应该有足够大的空间)。选中"自定义大小"单选按钮，在"初始大小(MB)"和"最大值(MB)"文本框中，分别输入虚拟交换文件大小的准确数值即可。

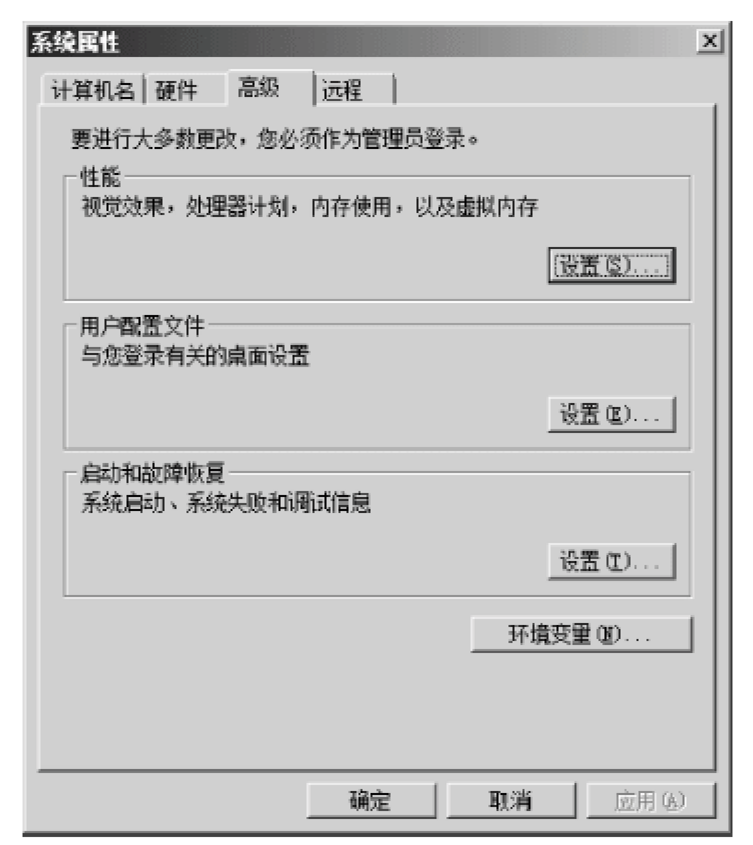


图3-28　"高级"选项卡



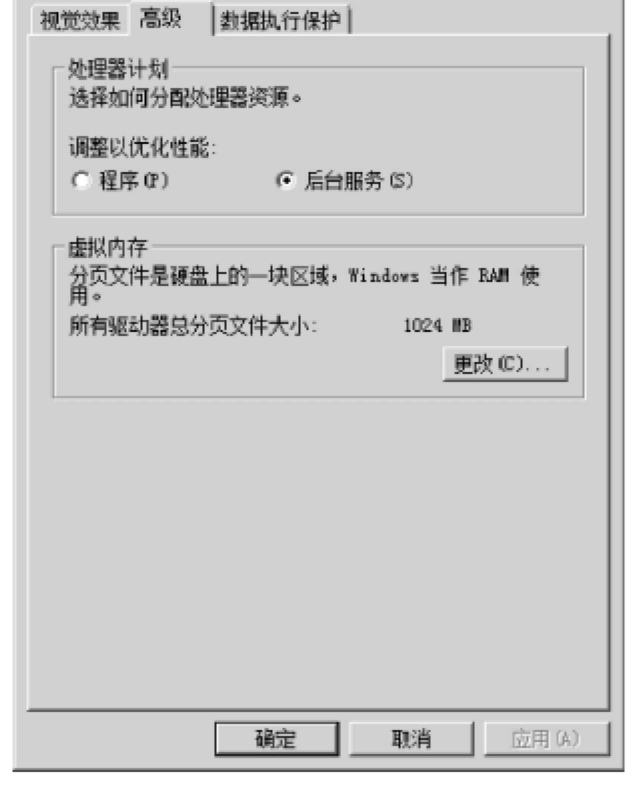


图3-29　"性能选项"对话框

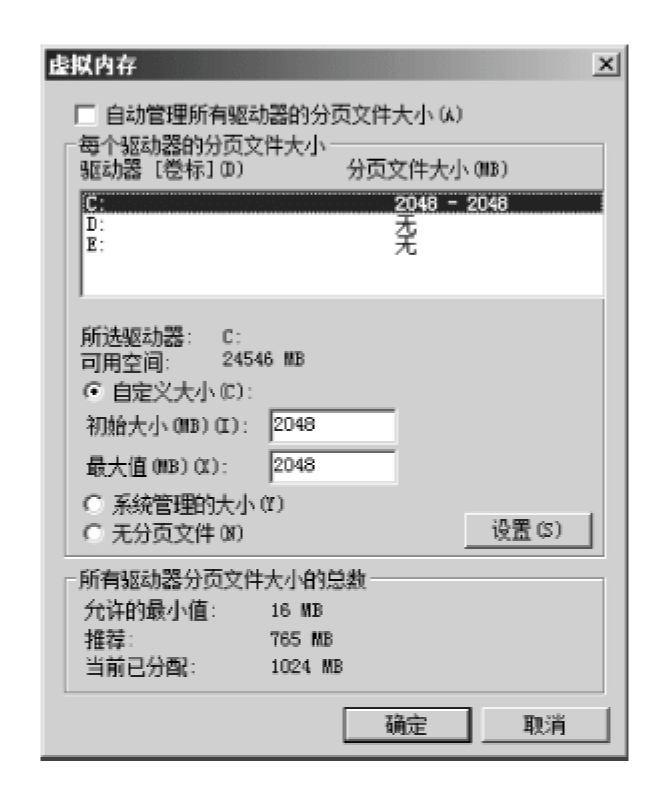


图3-30　设置虚拟内存

(4) 依次单击"确定"按钮，保存设置。并重新启动计算机，即可使设置生效。

3.4.2　系统变量的管理

系统变量由操作系统定义的数据存储位置，无论谁登录该计算机，该位置都是相同的。系统变量由Windows定义并应用到所有计算机用户。对系统环境的更改将写入注册表，而且通常需要重启计算机才能生效。

系统变量是环境变量的一部分，包含关于系统以及当前登录用户的环境信息的字符串，一些软件程序可以使用该信息确定临时文件夹的位置等。系统变量是系统中设置的变量，默认情况下系统变量不允许用户随便更改。

这里以修改TEMP缓存目录为例介绍具体设置系统变量的操作方法。

(1) 右击"计算机"图标，在快捷菜单中选择"属性"命令，打开"系统"窗口。在"任务"区域中，单击"高级系统设置"按钮，显示图3-31所示的"系统属性"对话框。

(2) 单击"环境变量"按钮，显示图3-32所示的"环境变量"对话框。在"系统变量"列表中，选择TEMP选项。

（3）单击“编辑”按钮，显示图 3-33 所示的“编辑系统变量”对话框。在“变量值”文本框中输入想要修改的变量值即可，这里修改值为 d:\TEMP。



图 3-32 “环境变量”对话框



图 3-31 “系统属性”对话框

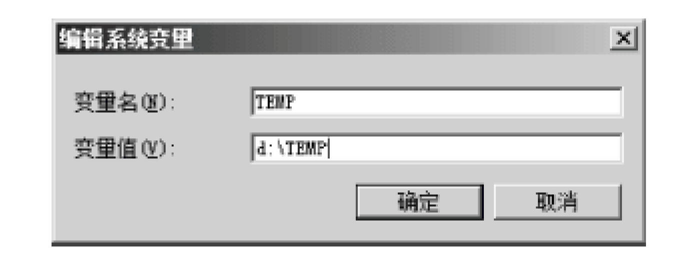


图 3-33 修改 TEMP 变量值

（4）单击“确定”按钮，保存设置即可。使用相同操作，可以修改其他系统变量。需要注意的是，有些系统变量可能会包括多个值，例如 PATH 变量，此时，可以使用英文输入状态下的分号(;)将多个变量分隔开。

3.5 可靠性和性能监视器

前面所讲的内容均是微软所提供的提高系统性能的方法，除此之外，在实际网络管理过程中，监控系统性能也是非常必要的。可靠性和性能监视器是 Windows Server 2008 内置的监控组件，将复杂的计数器监测数据以图表模式展示，最终结果为一张完整的图标或者一份完整的分析报告。管理员可以将生成的图表作为评测系统的性能基线，如果在非正常状态下计算机出现性能问题，通过比较即可发现问题的根源，加快排除故障的速度。

3.5.1 性能监视器

性能是用来评测计算机执行应用程序以及执行系统任务速度快慢的标准，从总体上讲，物理磁盘的访问速度、内存的可用性、处理器的速度以及网络带宽都会影响到系统性能。服务器在网络环境中的作用非常重要，特别需要管理员对其性能以及系统的可用性进行监测，确保服务器平稳运行。

1. 常用计数器

系统的整体性能由许多因素决定，例如 CPU 利用率、CPU 队列长度（即有多少任务正在等待 CPU 的服务）、磁盘忙闲程度（即磁盘驱动器有多少时间用于响应请求）、可用的物理内存、网络接口的利用情况等，表 3-4 所示为常用的性能计数器。

表 3-4　常用计数器

性能对象	计　数　器	提供的信息
Memory	Available Bytes	Available Bytes 显示出当前空闲的物理内存总量。当此数值变小时，Windows 开始频繁地调用磁盘页面文件。如果此数值很小，例如小于 5MB，系统会将大部分时间消耗在操作页面文件上
Memory	% Committed Bytes In Use	% Committed Bytes In Use 是 Committed Bytes 与 Commit Limit 之间的比值。Committed Memory 指如果需要写入磁盘时已在分页文件中保留空间的处于使用中的物理内存。Commit Limit 是由分页文件大小决定。如果扩大了分页文件，该比例就会减小。此计数器只显示当前百分比；而不是一个平均值
Memory	Page Faults/sec	Page Faults/sec 是指处理器处理错误页的综合速率。用错误页数/秒来计算。当处理器请求一个不在其工作集(在物理内存中的空间)内的代码或数据时出现的页错误。此计数器包括硬错误(那些需要磁盘访问的)和软错误(在物理内存的其他地方找到的错误页)。许多处理器可以在有大量软错误的情况下继续操作。但是，硬错误可以导致明显的拖延。此计数器显示用上两个实例中观察到的值之间的差除以实例间隔的持续时间所得的值
Network Interface	Bytes Total/sec	Bytes Total/sec 是发送和接收字节的速率，包括帧字符在内
Network Interface	Packets/sec	Packets/sec 为发送和接收数据包的速率
Physical Disk	% Busy Time	% Busy Time 指磁盘驱动器忙于为读取或写入请求提供服务所用的时间的百分比
Physical Disk	Avg. Disk Queue Length	Avg. Disk Queue Length 指读取和写入请求(为所选磁盘在实例间隔中列队的)的平均数
Physical Disk	Current Disk Queue Length	Current Disk Queue Length 指在收集操作数据时在磁盘上未完成的请求的数目。包括在快照内存时正在为其提供服务中的请求。这是一个即时长度而非一定间隔时间的平均值。多主轴磁盘设备可以一次有多个请求操作，但是其他同时发生的请求为等候服务。此计数器可能会反映一个暂时的高或低的列队长度，但是如果在磁盘驱动器存在持续负载，可能会长时间保持很高的值。请求等待时间与此列队的长度减去磁盘上的主轴成正比。此差值应小于 2 才能保持良好的性能
Processor	% Processor Time	% Processor Time 指处理器执行非闲置线程时间的百分比。此计数器设计成用来作为处理器活动的主要指示器。它通过在每个范例间隔中衡量处理器用于执行闲置处理线程的时间，并且用 100% 减去该值得出(每个处理器有一个闲置线程，该线程在没有其他线程可以运行时消耗周期)，可将其视为范例间隔用于做有用工作的百分比
Processor	% User Time	% User Time 指用于用户模式的非闲置处理器时间的百分比(用户模式是为应用程序、环境分系统和整数分系统设计的有限处理模式。另一个模式为特权模式，是为操作系统组件设计的并且允许直接访问硬件和所有内存。操作系统将应用程序线程转换成特权模式以访问操作系统服务)。此计数值将平均忙时作为实例时间的一部分显示
Server Work Queues	Queue Length	Queue Length 指 CPU 当前的服务器作业队列长度。队列长度长时间超过时可能表示处理器堵塞。此值为即时计数，不是一段时间的平均值

续表

性能对象	计　数　器	提供的信息
System	Processor Queue Length	Processor Queue Length 是指处理队列中的线程数。即使在有多个处理器的计算机上处理器时间也会有一个单队列。与磁盘计数器不同，该计数器仅计数就绪的线程，而不计数运行中的线程。如果处理器队列中总是有两个以上的线程通常表示处理器堵塞。此计数器仅显示上一次观察的值；而不是一个平均值
TCP	Segments Retransmitted/sec	Segments Retransmitted/sec 指程序段重新传输的速率，即传输的程序段中包含一个或多个以前传输过的字节

2. 启动性能监视器

Windows Server 2008 中提供了多种启动性能监视器的方法，常用的启动方法是命令行模式和图形模式。

(1) 图形模式启动方法

依次选择“开始”→“管理工具”→“可靠性和性能监视器”命令，显示“可靠性和性能监视器”窗口。依次展开“可靠性和性能”→“监视工具”→“性能监视器”目录，即可显示“性能监视器”窗口，如图 3-34 所示。

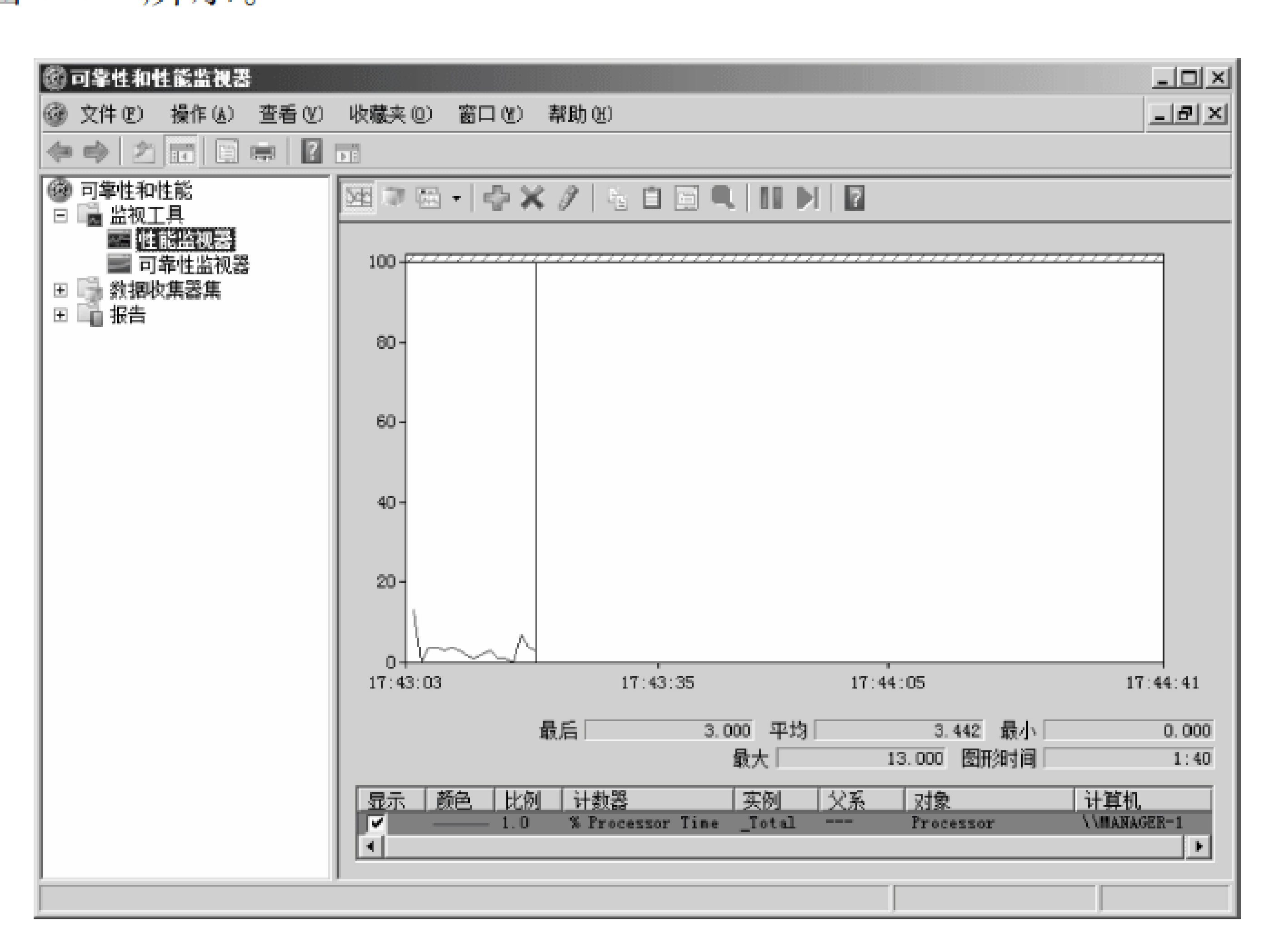


图 3-34 “性能监视器”窗口

另外，“性能监视器”窗口还可以在“服务器管理器”窗口中打开，依次选择“开始”→“服务器管理器”命令，打开“服务器管理器”窗口，依次展开“服务器管理器”→“诊断”→“可靠性和性能”→“监视工具”→“性能监视器”目录即可，如图 3-35 所示。

(2) 命令行模式启动方法

① 依次选择“开始”→“运行”命令，打开“运行”对话框，在“打开”文本框中输入 perfmon/sys，如图 3-36 所示。

② 单击“确定”按钮，启动“性能监视器”窗口，如图 3-37 所示。

3. 管理性能监视器

性能监视器通常是在 MMC 控制台窗口打开，而实际上是通过性能计数器监视计算机

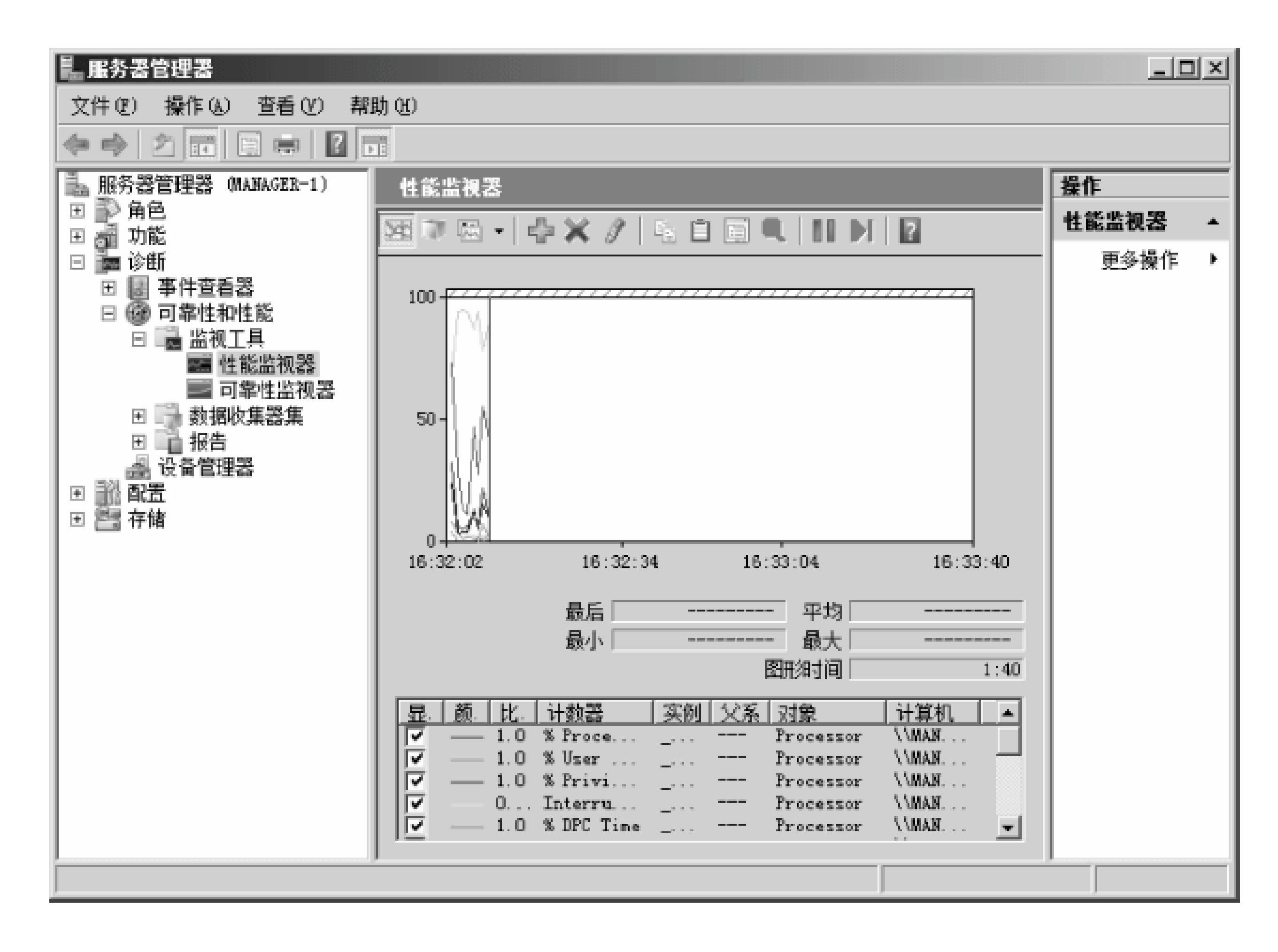


图 3-35 性能监视器



图 3-36 “运行”对话框

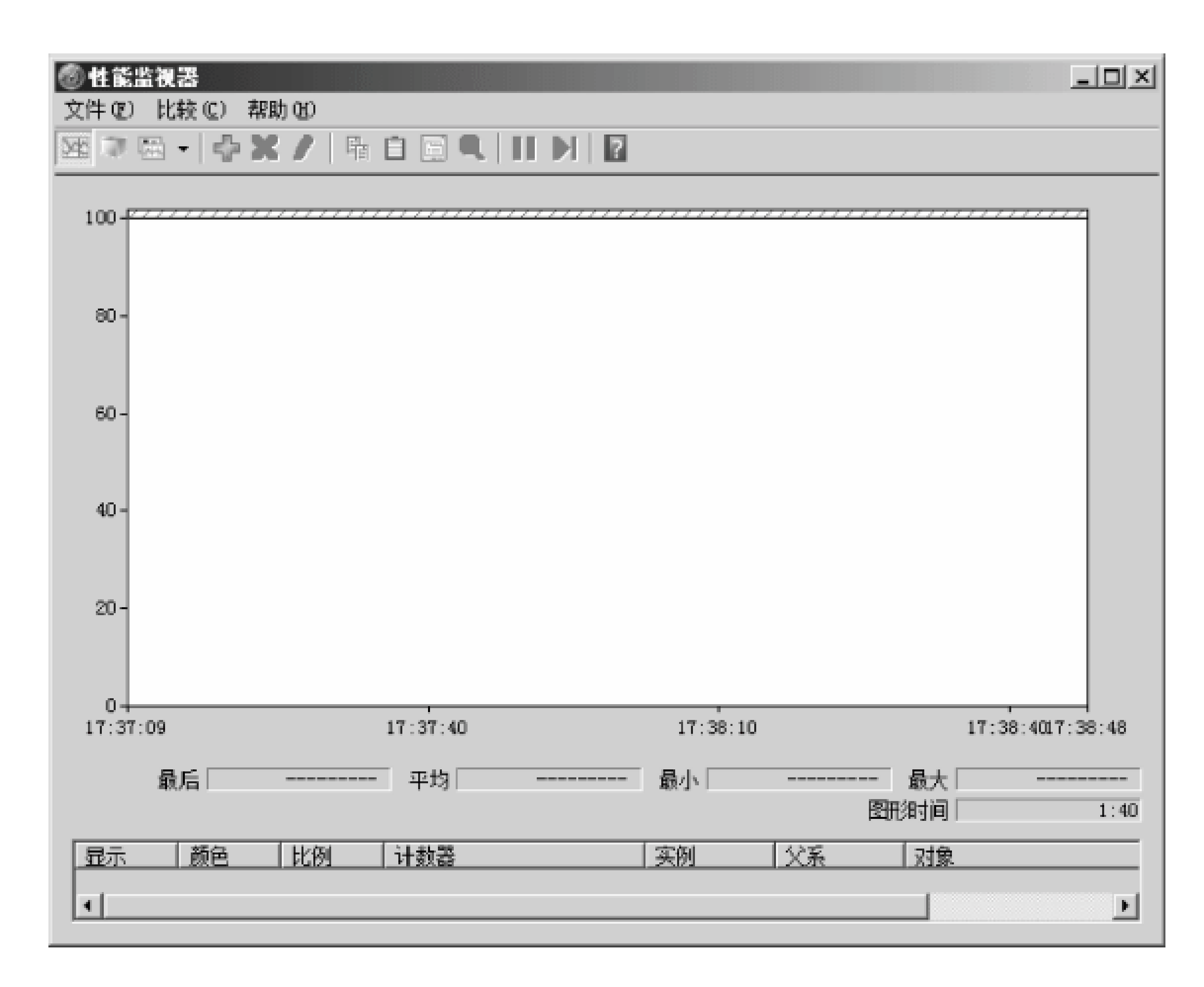


图 3-37 使用命令启动性能监视器

系统的性能，通过连续跟踪产生图表，根据图表即可查看计算机的性能。性能监视器具体常用的管理任务如下。

（1）添加计数器

计数器是衡量计算机性能的重要指标，默认状态下没有部署任何计数器，在 Windows Server 2008 中添加所有组件计数器的方法相同，这里以添加监控 CPU 计数器为例说明如何添加计数器。

① 在“性能监视器”窗口中单击 按钮，显示“添加计数器”对话框。在“可用计数器”区域的“从计算机选择计数器”下拉列表框中选择需要监视的目标计算机，本例中选择“本地计算机”。在“从计算机选择计数器”列表中选择 Processor 选项，单击 按钮，展开该选项的所有计数器，如图 3-38 所示。

② 选择目标计数器，在“选定对象的实例”列表中选择目标实例。如果选择“所有实



图 3-38 “添加计数器”对话框

例”选项，则监视目标计算机中的所有 CPU 对象。如果存在多个 CPU，在列表中显示 CPU 的索引号，例如 0、1。选择“0”表示选择第一个 CPU，选择“1”表示选择第 2 个 CPU。

③ 单击“添加”按钮，将选择的计数器添加到“添加的计数器”列表中，如图 3-39 所示。如果需要删除计数器，在“添加的计数器”列表中，选择需要删除的计数器，单击“删除”按钮即可。

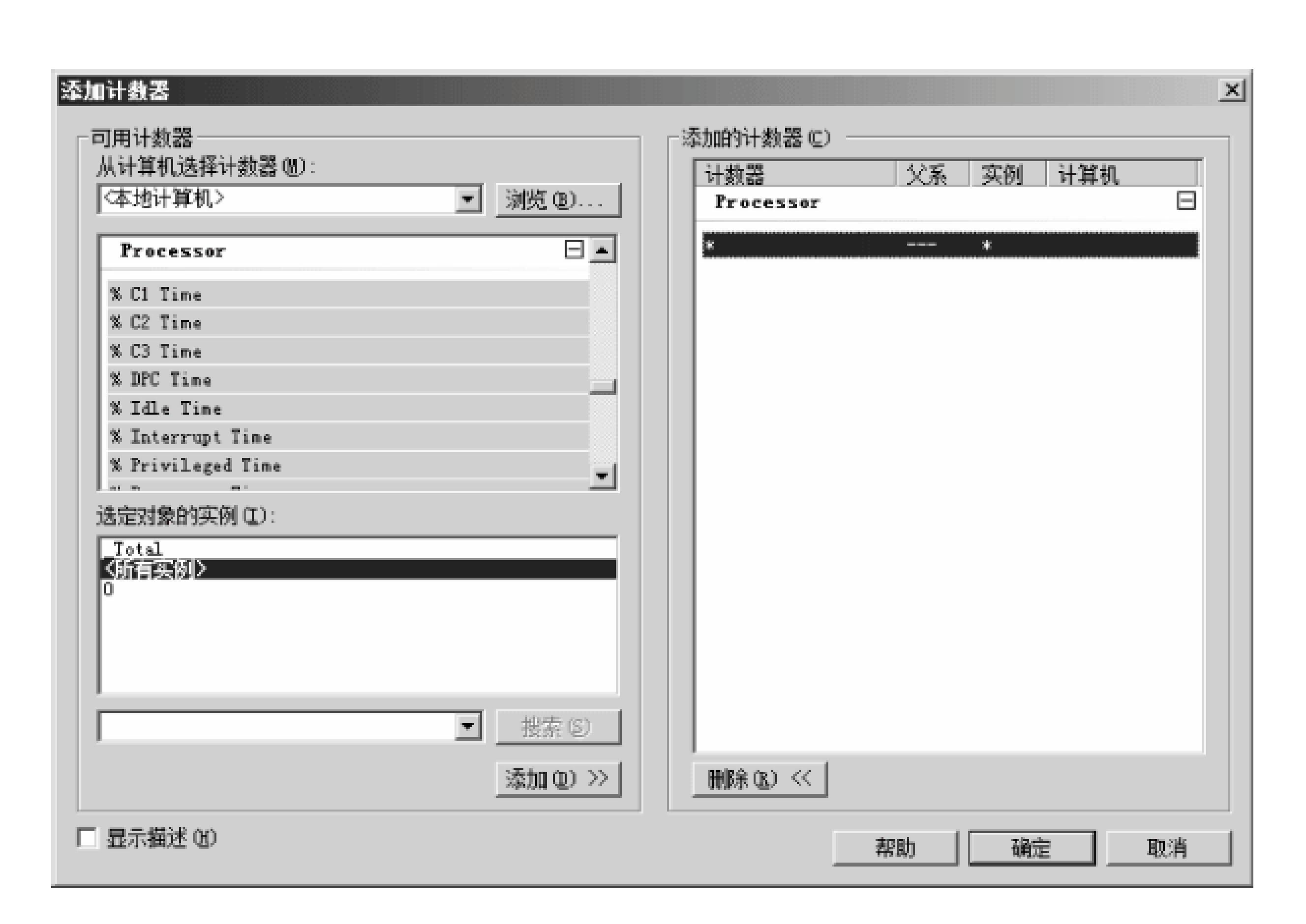


图 3-39 成功添加计数器

④ 单击“确定”按钮，选择的计数器添加到监视图表中，自动启动该性能计数器，开始监视计算机的性能，如图 3-40 所示。

（2）调整图表显示

性能计数器默认显示模式为“线条”，管理员还可以根据个人习惯修改模式为“直方图”和“报告”。具体操作步骤如下：在“性能监视器”窗口中，单击 按钮，可以选择计数器的显示模式。选择“直方图”选项，显示图 3-41 所示的窗口；选择“报告”选项，显示图 3-42 所示的窗口。

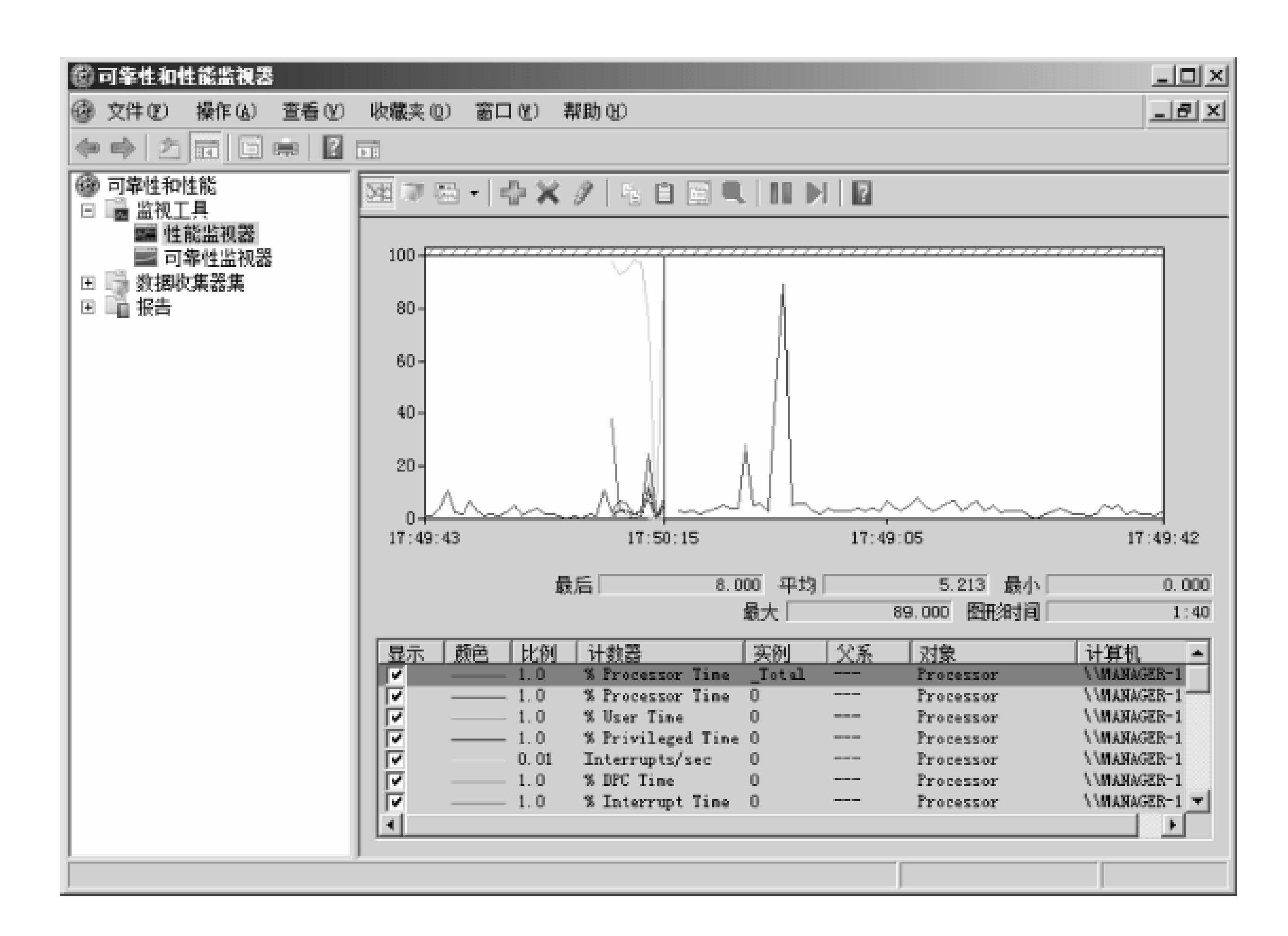


图 3-40 开始使用新添加的计数器

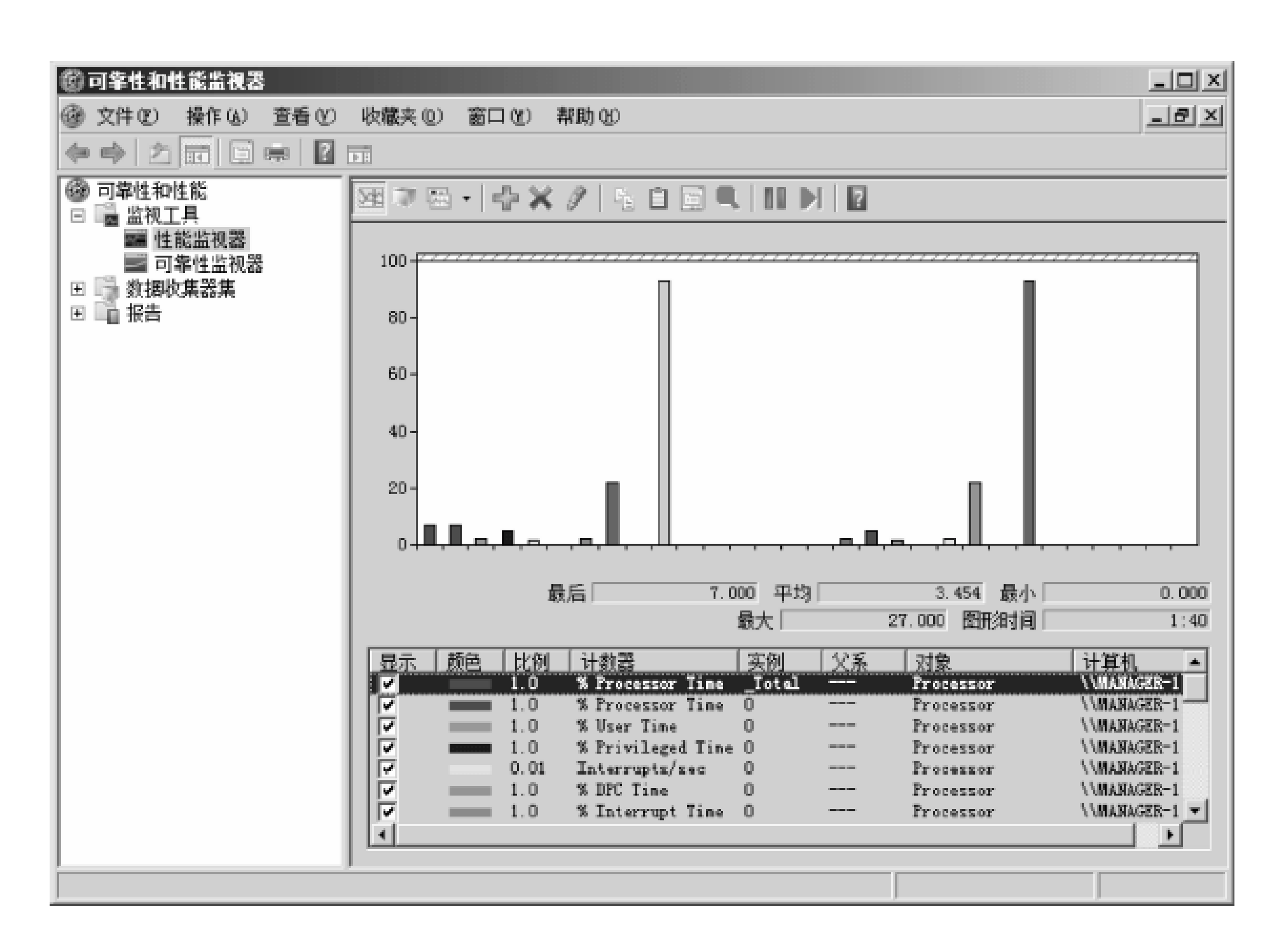


图 3-41 “直方图”显示模式



图 3-42 “报告”显示模式

(3) 删除计数器

对于某些无效的计数器，需要将其删除。具体操作步骤如下：选择目标计数器(颜色为绿色)，单击✖按钮，即可删除选择的计数器。

(4) 突出显示计数器

在实际使用过程中，可能会同时启用多个被监视的计数器，如果管理员需要查看其中的一个计数器，可以使用“突出显示”功能，查看选择的计数器。

选择目标计数器，单击🖉按钮，监视窗口中选择的计数器，所选中的计数器将以加粗黑线条显示，如图 3-43 所示。

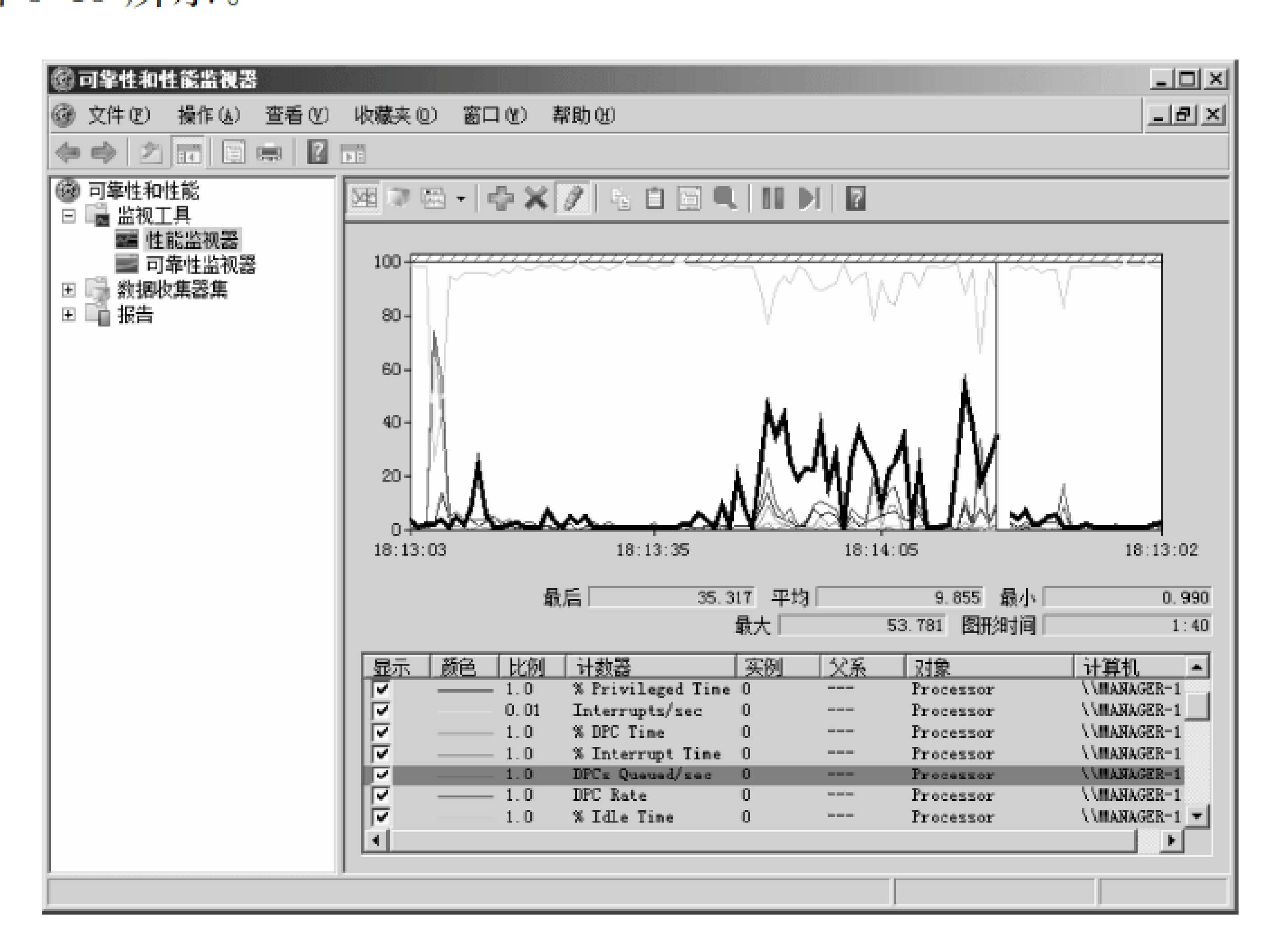


图 3-43　突出显示计数器

(5) 冻结显示

冻结显示完成的功能是停止监视计数器，保持当前的状态。需要注意的是，该功能将停止监视所有的计数器。

选择目标计数器(颜色为绿色)，单击⏸按钮，冻结选择的计数器，如图 3-44 所示。命令执行后，将不再动态监视启用的计数器。

(6) 隐藏计数器

如果监视的计数器过多，将不利于管理、分析计算机的当前状态，此时，可以在图表中隐藏部分不常用的计数器，只保留特别需要关注的计数器。

在“性能监视器”窗口中，选择需要隐藏的目标计数器，在监视图表中右击要隐藏的计数器，在快捷菜单中选择“隐藏选中的计数器”命令，即可隐藏所选择的计数器。

(7) 存储监视图像

因为监视图表可以作为衡量服务器性能的参考资料，因此需要将这些监视图像保存到磁盘中，以备日后使用。

在监视图表中右击，在快捷菜单中选择“图像另存为”命令，显示图 3-45 所示的“另存为”对话框，输入文件名并设置图片格式。单击“保存”按钮，即可将当前的监视图表保存为图片，默认图片格式为 GIF 格式。

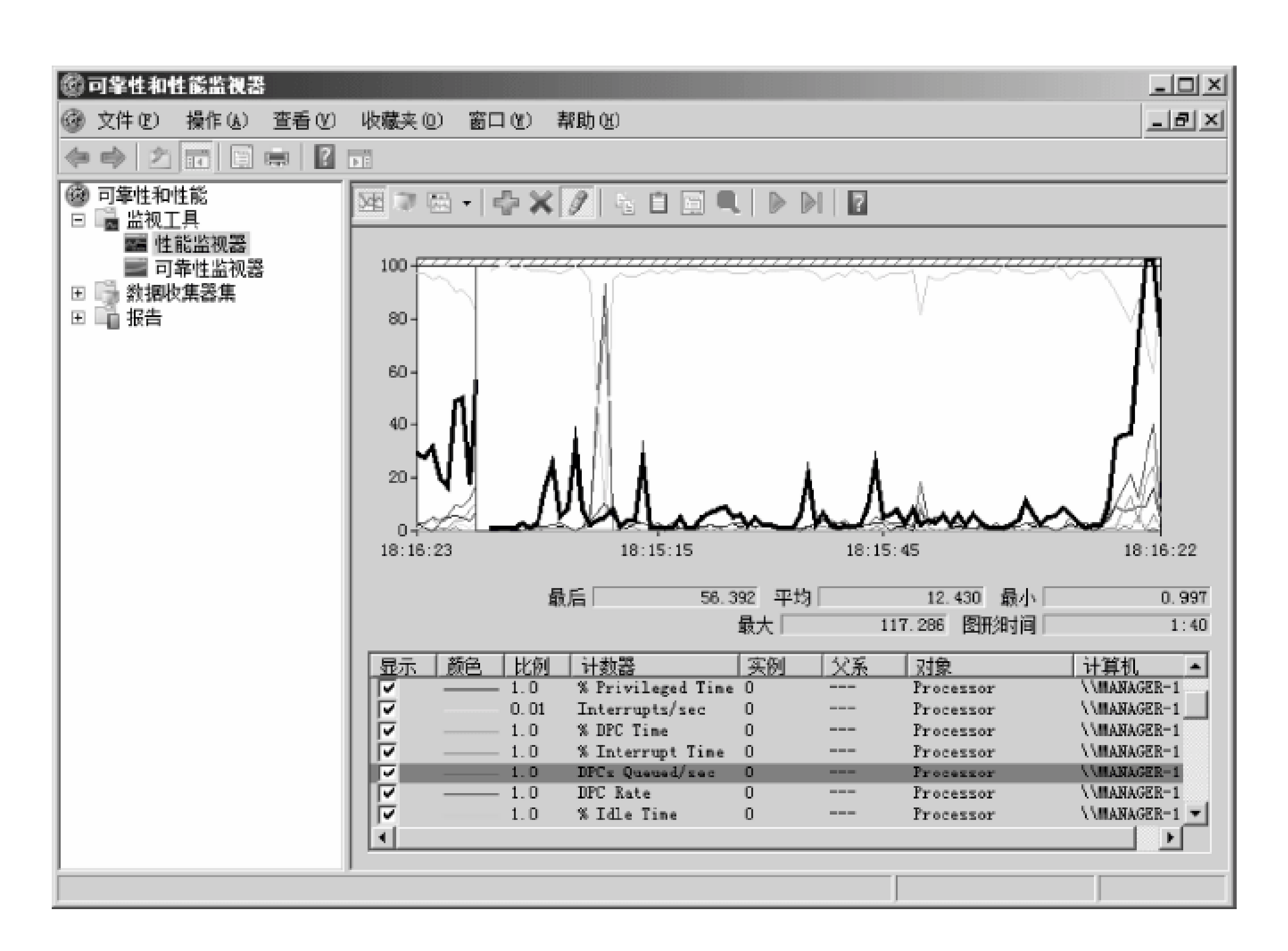


图 3-44　冻结显示

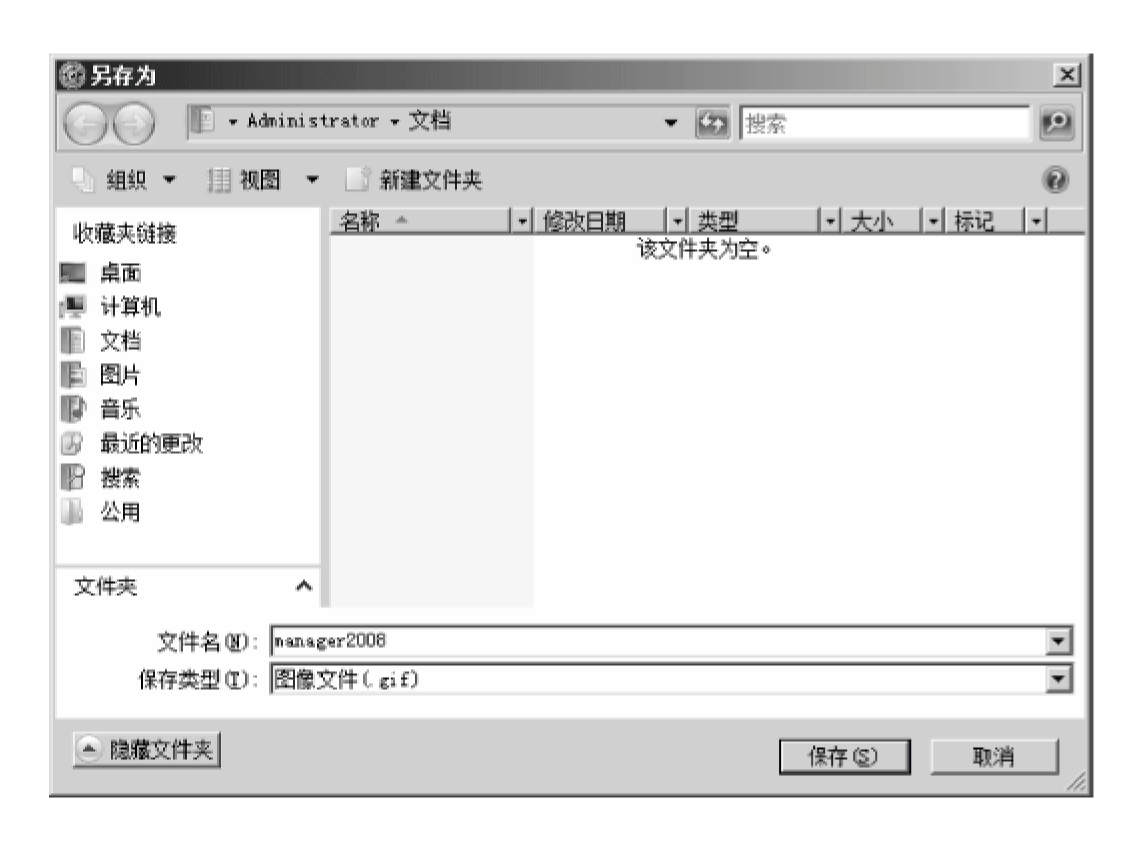


图 3-45　存储监视图像

3.5.2　可靠性监视器

可靠性监视器是 Windows Server 2008 操作系统内置监视功能，通过该功能管理员可以了解服务器系统运行状况。从 Windows Server 2008 操作系统安装成功时开始，每隔 24 个小时，系统就会对统计出来的数据内容进行统计，并自动生成一个系统稳定性系数，通常该系数数值位于 0～10 之间，数值越高说明系统的可靠性越高，该系数数值将自动显示在可靠性图表中。Windows Server 2008 操作系统自动对 Windows 故障、硬件故障、应用程序故障、软件安装（卸载）以及其他故障进行可靠性统计。当可靠性监视器连续收集 28 天的数据后，可靠性监视器图表将显示一条使用黑色方块节点串联起来的实线，显示计算机在一段时间区域内的运行状况。

1．可靠性监视器概述

“可靠性监视器”窗口包含两个显示区域，上面区域是“系统稳定性图表”，下面区域为“系统稳定性报告”，显示系统自动统计的关联数据。

(1) 系统稳定性图表

系统稳定性图表的上半部分显示稳定性系数图表。在该图表的下半部分显示跟踪的可靠性事件,该事件将有助于系统的稳定性测量,或者提供有关软件安装和删除的相关信息。当检测到每种类型的一个或多个可靠性事件时,在该日期的列中会显示一个图标,如图 3-46 所示。图标的具体含义如下。

① 信息图标,该图标所在的位置表示在该位置有操作成功的提示信息存在。

② 警告图标,该图标所在的位置表示在该位置有安全隐患操作存在。

③ 错误图标,该图标所在的位置表示在该位置有错误操作存在。

④ 黑色方块图标,该图标所在的位置表示每一天的事件采集点,每一个事件采集点包含 5 个方面的信息,分别是:Windows 故障信息、硬件故障信息、应用程序故障信息、软件安装(卸载)信息、其他故障信息。

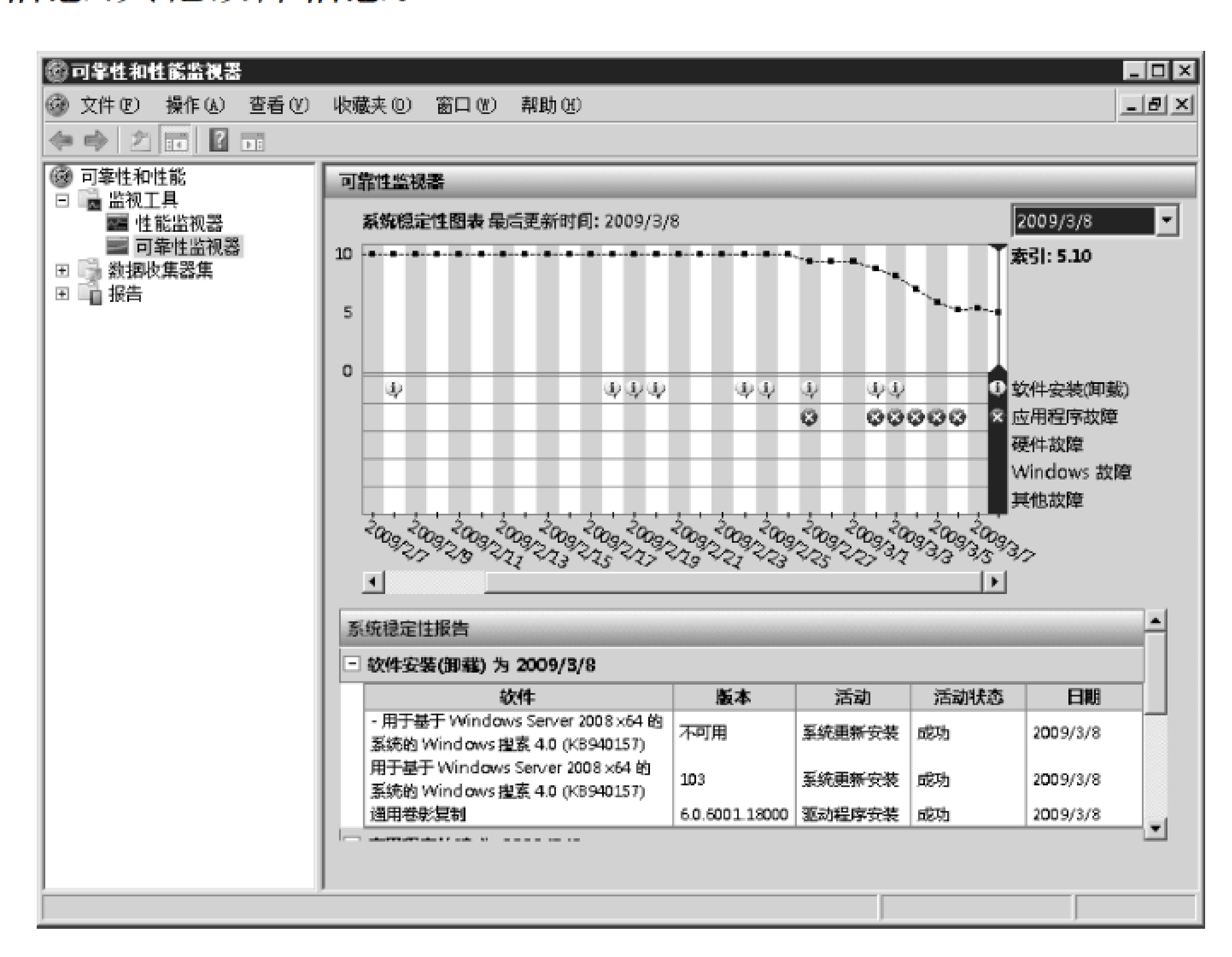


图 3-46 系统稳定性图表

Windows Server 2008 操作系统自动对每一个事件采集点收集来的 5 个方面信息进行综合评估,并对系统的运行稳定性进行量化评估,其中最稳定的系统状态,其可靠性的评估分为 10 分。随着系统运行时间的推移,系统运行的可靠性将逐步下降。

默认情况下,可靠性监视器显示最近日期的数据。若要查看特定日期的数据,选择系统稳定性图表中的"日期",或者单击日期下拉列表框选择"选择日期"选项,在日期列表中选择目标日期,如图 3-47 所示。

若要查看所有可用的历史数据,单击日期下拉列表框选择"全部"选项,即可显示所有日期可靠性监视结果。如果采集的数据超过 30 天,则使用系统稳定性图表底部的滚动栏,浏览可见范围以外的日期。

(2) 系统稳定性报告

系统稳定性报告能够帮助管理员通过识别产生的事件确定造成系统稳定性降低的原因。单击每个可靠性事件类别左侧的+图标,可以查看事件列表。如果选择系统稳定性图

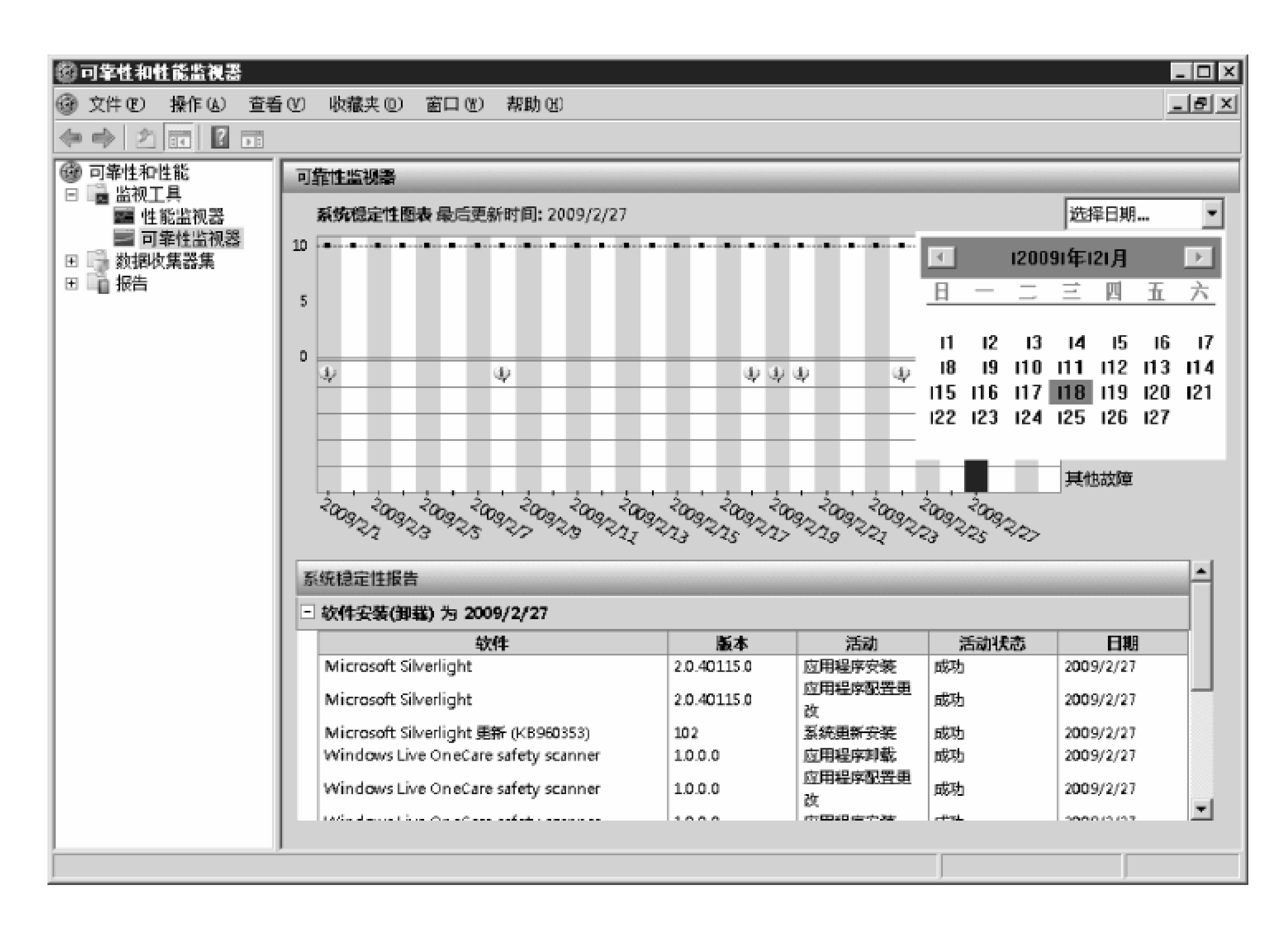


图 3-47 选择日期

表中的日期列，则系统稳定性报告将显示该日期的事件。若要查看系统稳定性图表中的所有事件或选择可见范围以外的日期，选择日期下拉列表框并使用日历，或选择“所有日期”选项，查看选择的时间区间产生的与可靠性相关的事件。系统稳定性报告包括以下 5 种类型的事件，分别是：软件安装(卸载)、应用程序故障、硬件故障、Windows 故障以及其他故障。

2. 启动可靠性监视器

启动可靠性监视器与启动性能监视器相似，同样可以通过命令行模式和图形模式启动。

(1) 命令行模式

打开“运行”对话框，在“打开”文本框中输入 perfmon，单击“确定”按钮，显示图 3-48 所示的“可靠性和性能监视器”窗口。依次选择“可靠性和性能”→“监视工具”→“可靠性监视器”选项，即可显示“可靠性监视器”窗口。

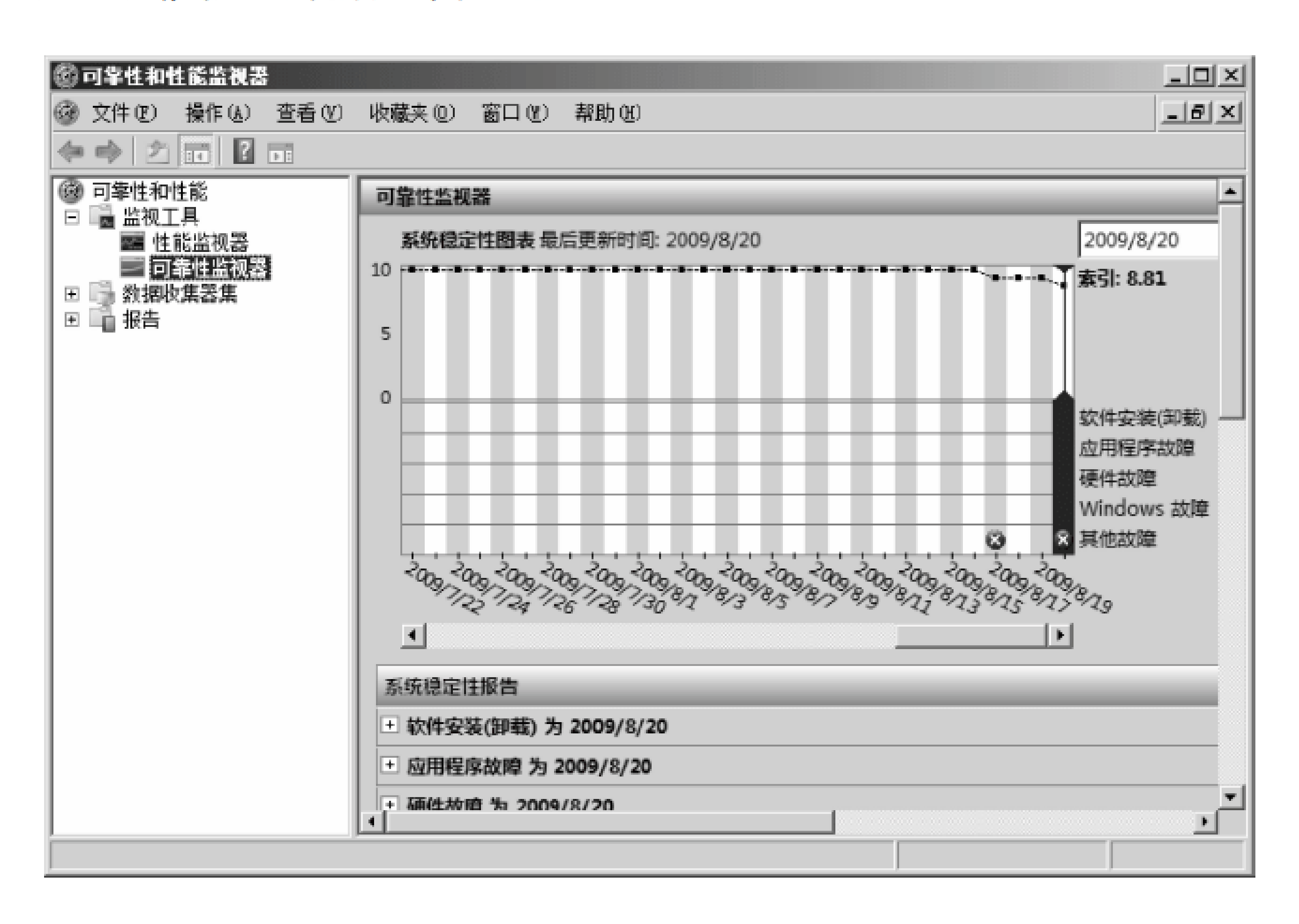


图 3-48 “可靠性和性能监视器”窗口

（2）图形模式

依次选择"开始"→"管理工具"→"可靠性和性能监视器"命令，打开"可靠性和性能监视器"窗口。依次展开"可靠性和性能"→"监视工具"→"可靠性监视器"目录，即可显示"可靠性监视器"窗口。

3. 监控系统数据

Windows Server 2008 的可靠性监视器，自动监控 Windows 故障、硬件故障、应用程序故障、软件安装（卸载）以及其他故障类别的错误，当错误发生后，管理员通过可靠性图表即可发现并捕捉产生的错误，了解错误产生的原因。

（1）监控指定日期数据

在"可靠性监视器"窗口选择某一天的可靠性系数后，在"系统稳定性报告"区域看到对应这一天的详细统计数据，如图 3-49 所示。管理员可以监控选择的计算机是否出现 Windows 故障，是否存在硬件故障，应用程序在使用过程中是否发生过意外，有没有进行过软件安装操作或者卸载操作等，依照统计结果，管理员可以在第一时间采取措施保护服务器操作系统安全，例如升级硬件驱动程序，及时更新 Windows 系统补丁程序，或者将存在稳定性隐患的软件及时从系统中卸载等。

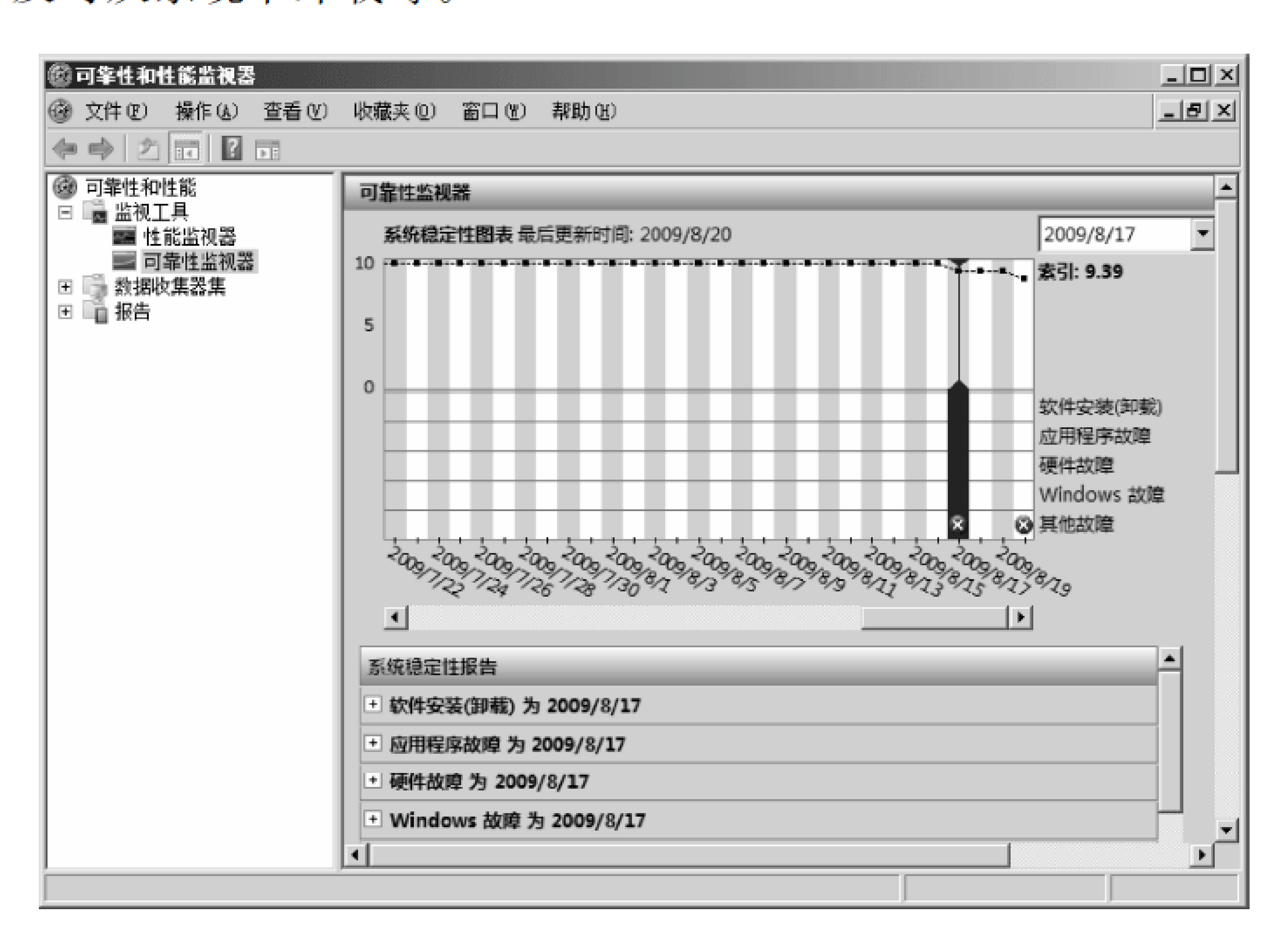


图 3-49 监控指定日期数据

（2）监控软件安装（卸载）

在"系统稳定性报告"区域，选择"软件安装（卸载）"选项，单击该选项左侧的＋图标，显示指定日期发生的软件安装（卸载）行为。

（3）监控应用程序故障

在"系统稳定性报告"区域，选择"应用程序故障"选项，单击该选项左侧的＋图标，可以查看指定日期应用程序出现的故障。

（4）监控硬件故障

在"系统稳定性报告"区域，选择"硬件故障"选项，单击该选项左侧的＋图标，可以查看指定日期计算机硬件出现的故障。

(5) 监控 Windows 故障

在“系统稳定性报告”区域，选择“Windows 故障”选项，单击该选项左侧的＋图标，可以查看指定日期 Windows 操作系统出现的故障。

(6) 监控其他故障

在“系统稳定性报告”区域，选择“其他故障”选项，单击该选项左侧的＋图标，可以查看指定日期系统中出现的其他故障。

3.5.3 数据收集器

数据收集器集是 Windows 可靠性和性能监视器中性能监视和报告的功能模块，可以将多个数据收集点组织成可用于查看或记录性能的单个组件。数据收集器集是数据收集器的集合，而数据收集器是各种计数器的集合。数据收集器收集到的数据信息将自动记录到日志中，管理员既可以在 Windows 性能监视器中查看，也可以选择通过其他非 Microsoft 应用程序查看。

1. 启动数据收集器

在 Windows Server 2008 操作系统中，管理员可以通过命令行模式和服务器管理器启动数据收集器。其启动的两种方法同启动可靠性监视器，具体操作方法参见前面相关内容，这里就不再赘述。在“可靠性和性能监视器”窗口中，依次展开“可靠性和性能”→“数据收集器集”目录，即可打开“数据收集器集”窗口，如图 3-50 所示。

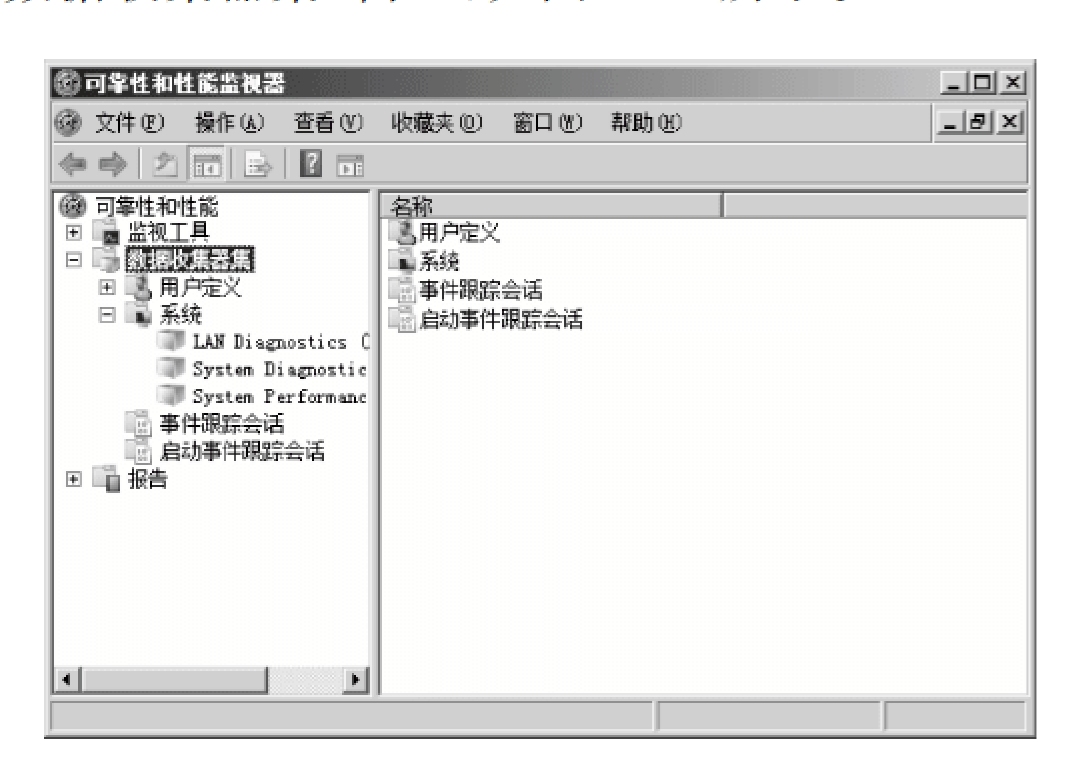


图 3-50 “数据收集器集”窗口

2. 系统诊断

Windows Server 2008 的数据收集器集中，集成“系统诊断”功能，管理员启动该功能后，即可对计算机的健康状态进行诊断，诊断的结果以报表方式显示。系统诊断详细记录本地硬件资源的状态、系统响应时间和本地计算机上的进程，还包含系统信息和配置数据等信息。

1) 启动系统诊断

(1) 打开“数据收集器集”窗口，依次选择“系统”→“System Diagnostics(系统诊断)”选项，如图 3-51 所示。在右侧列表中，显示集成的计数器、性能参数、配置信息等。

(2) 右击“System Diagnostics(系统诊断)”选项，在快捷菜单中选择“开始”命令，开始诊断系统的健康状态。右击“System Diagnostics(系统诊断)”选项，在快捷菜单中选择“最



图 3-51 System Diagnostics(系统诊断)

新的报告"命令,显示图 3-52 所示的"系统诊断"窗口,显示当前的"报告状态"为"收集数据"。



图 3-52 "系统诊断"窗口

2)系统诊断报告

系统诊断数据采集完成后,自动停止采集任务,此时将为管理员提供详细的系统健康报告。

(1)采集任务完成后,右击"System Diagnostics(系统诊断)"选项,在快捷菜单中选择"最新的报告"命令,打开"系统诊断报告"窗口。单击"诊断结果"任务条,显示计算机的健康状态,如图 3-53 所示。

① 在"错误"选项区域中,显示计算机中检测到的错误信息,例如服务异常,没有安装驱动程序等。详细的显示错误的症状、原因、详细信息、分辨率以及相关站点(提供当前症状的解决方案)。



图 3-53 诊断结果

② 在“信息”选项区域中，显示计算机中检测到的警告性信息，如图 3-54 所示。详细显示错误的症状、原因、分辨率以及相关站点（提供当前症状的解决方案）。

③ 在“基本系统检查”选项区域中，显示计算机系统检查信息，包括 OS 检查、硬盘检查、安全中心测试、系统服务检查以及硬件设备和驱动程序检查，如图 3-55 所示。检查通过显示的结果为●，检查失败显示的结果为●。单击“磁盘检查”左侧的＋图标，显示所有磁盘的检查状态。

④ 在“性能”选项区域中，显示计算机的性能，包括 CPU、网络、磁盘以及内存的利用率和详细信息，如图 3-56 所示。

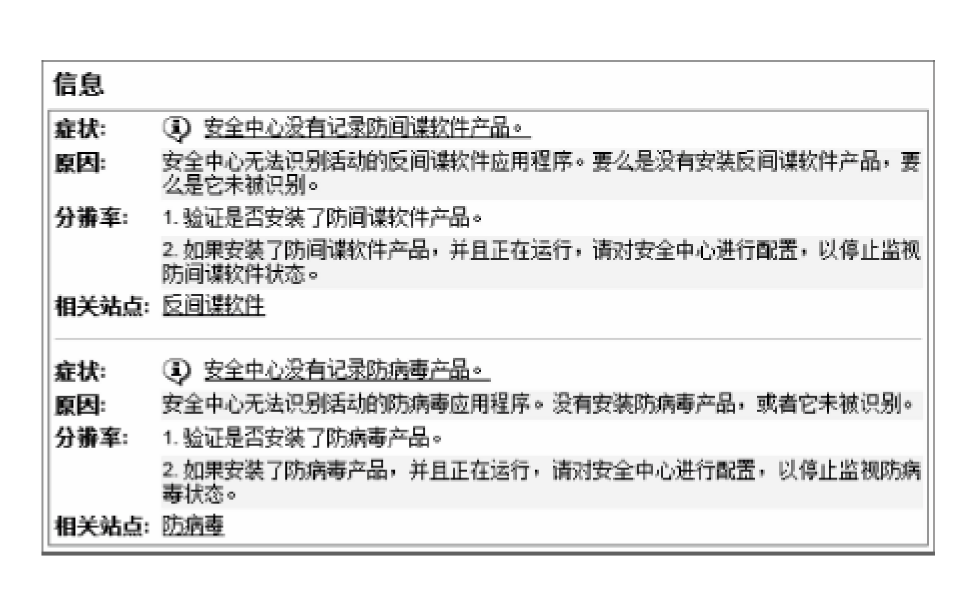


图 3-54 “信息”选项区域



图 3-55 “基本系统检查”选项区域

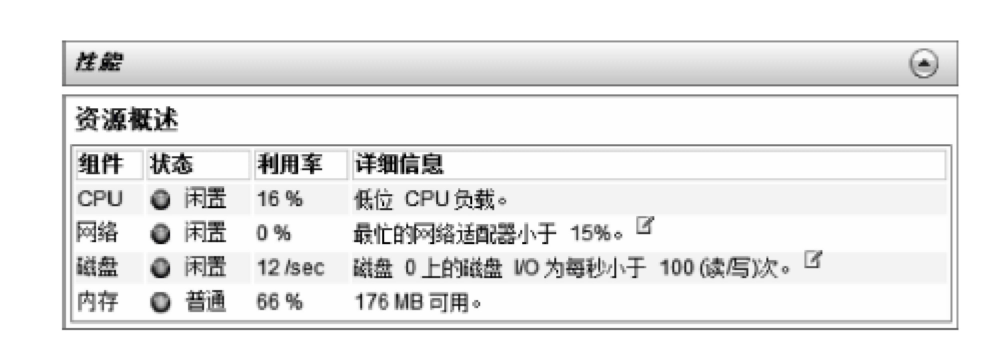


图 3-56 “性能”选项区域

（2）使用相同的方法，可以查看诊断的其他任务结果，包括软件配置、硬件配置、CPU、网络、磁盘以及内存等信息，如图 3-57 所示。

3. 系统性能监控

Windows Server 2008 的数据收集器集中，集成“系统性能”功能，管理员启动该功能后，即可对计算机进行监控，监控的结果以报表方式显示。“报告”功能是 Windows Server 2008 系统可靠性和性能监视器的新增功能之一，主要用于直观反映数据收集器集的工作状



图 3-57　全部诊断信息

态和结果。默认情况下，所有数据收集器集都可以在“报告”项目中，找到与之对应的数据收集器集报告。使用“报告”功能时，应注意如下几个方面。

(1) 如果数据收集器集未运行，将没有可用的报告。

(2) 如果数据收集器集正在运行，则控制台窗口中将显示有关数据收集器集被配置为运行多长时间的信息，无法查看历史记录。

(3) 数据收集停止之后，生成报告时会有一段延迟。这段时间期间，控制台窗口将显示工作图标。

(4) 较大的日志文件将使生成报告的时间较长。如果频繁检查日志以查看最新数据，建议使用限制以自动分段日志。可以使用 relog 命令对长日志文件进行分段或合并多个短日志文件。

系统性能数据采集完成后，会自动停止采集任务，并为管理员提供详细的系统性能报告。

(1) 采集任务完成后，右击“System Performance(系统性能)”选项，在快捷菜单中选择“最新的报告”命令，打开“系统性能报告”窗口。

(2) 单击“摘要”任务条，显示“进程”、“磁盘”、“内存”的利用率，如图 3-58 所示。

(3) 单击“诊断结果”任务条，显示计算机的系统性能，如图 3-59 所示。根据提供的参数即可了解当前计算机的性能。

(4) 单击“CPU”、“网络”、“磁盘”、“内存”任务条，将详细显示在监控中监控的详细信息。管理员可以根据需要查看关心的数据和内容。

4. 自定义性能数据器集

Windows Server 2008 提供自定义数据收集器功能，管理员可以使用模板(系统诊断、系统性能)派生新的收集器，也可以创建全新的收集器，本例以创建全新的性能数据收集器为例说明如何创建新的监控指标。

(1) 创建性能数据器集

① 打开“数据收集器集”窗口，右击“用户定义”选项，在快捷菜单中选择“新建”命令，在



图 3-58 摘要信息



图 3-59 诊断结果

级联菜单中选择“数据收集器集”命令。启动“创建新的数据收集器集”向导，显示图 3-60 所示的“您希望以何种方式创建这一新的数据收集器集”对话框。定义新收集器集的名称，并选择数据收集器集的创建类型。本例中选中“手动创建(高级)”单选按钮。

② 单击“下一步”按钮，显示图 3-61 所示的“您希望包括何种类型的数据”对话框。选中“创建数据日志”单选按钮，并选中“性能计数器”复选框。

③ 单击“下一步”按钮，显示“您希望记录哪个性能计数器”对话框。单击“添加”按钮，在“可用计数器”列表中，选择并展开 Paging File 选项，选择%Usage 计数器，单击“添加”按钮，将选择的计数器添加到“添加的计数器”列表中。单击“确定”按钮，关闭计数器选择对话框，返回到“您希望记录哪个性能计数器”对话框，成功添加计数器，如图 3-62 所示。根据需要在“示例间隔”和“单位”文本框中，输入计数器的采样间隔时间和时间单位。

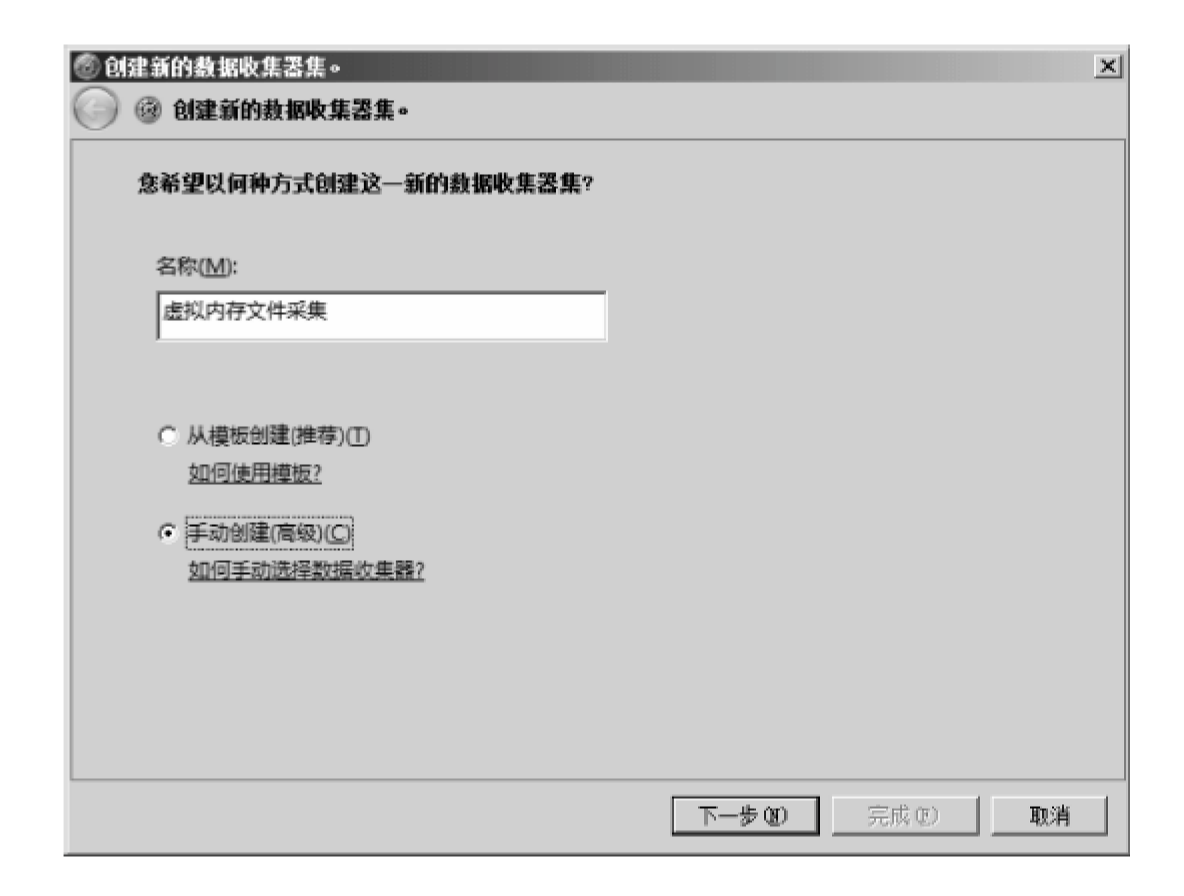


图 3-60 “您希望以何种方式创建这一新的数据收集器集”对话框



图 3-61 “您希望包括何种类型的数据”对话框

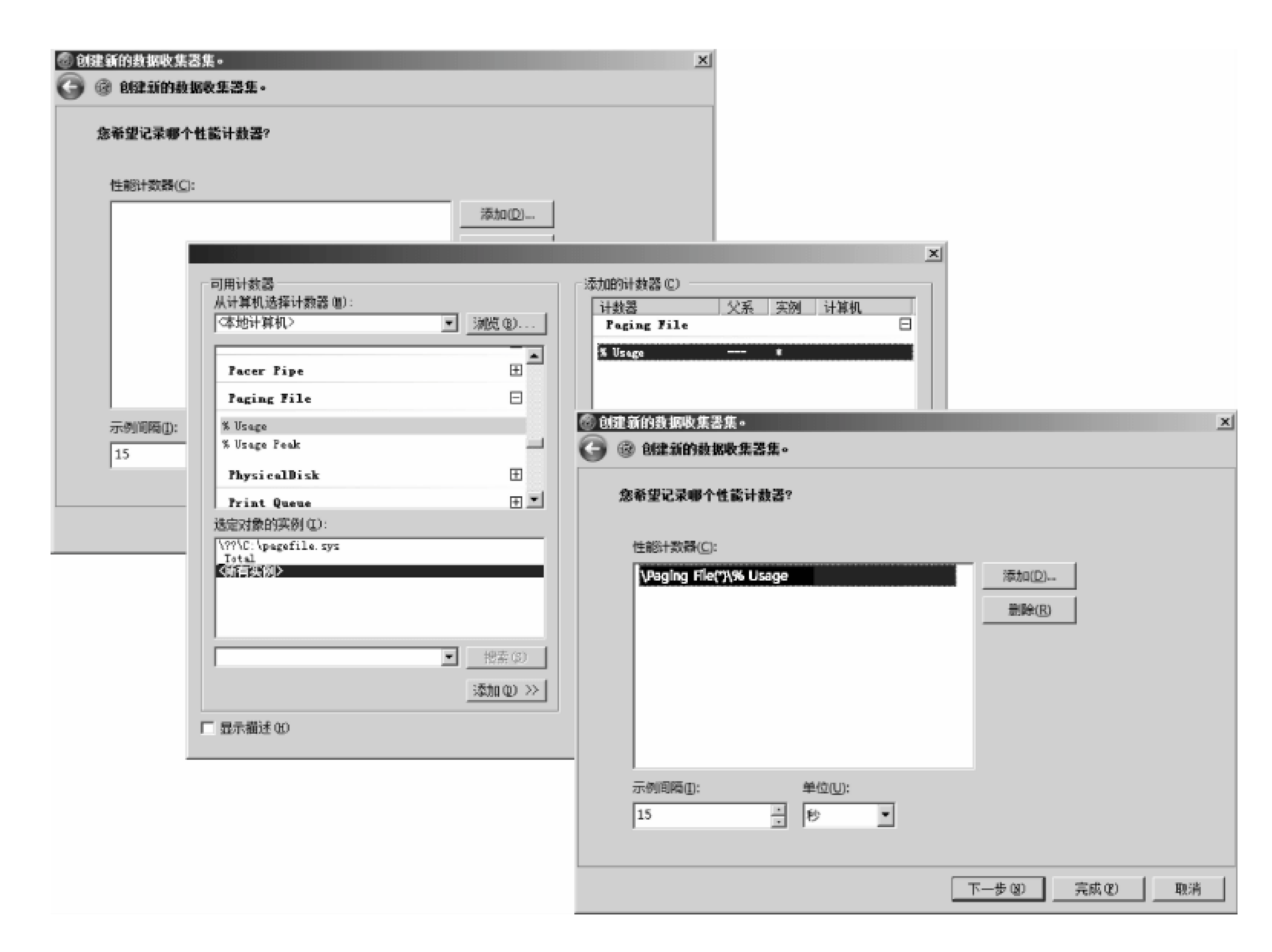


图 3-62 添加计数器

④ 单击“下一步”按钮，显示图 3-63 所示的“您希望将数据保存在什么位置”对话框。设置采集的数据文件存储目标文件夹，这里保持默认设置。

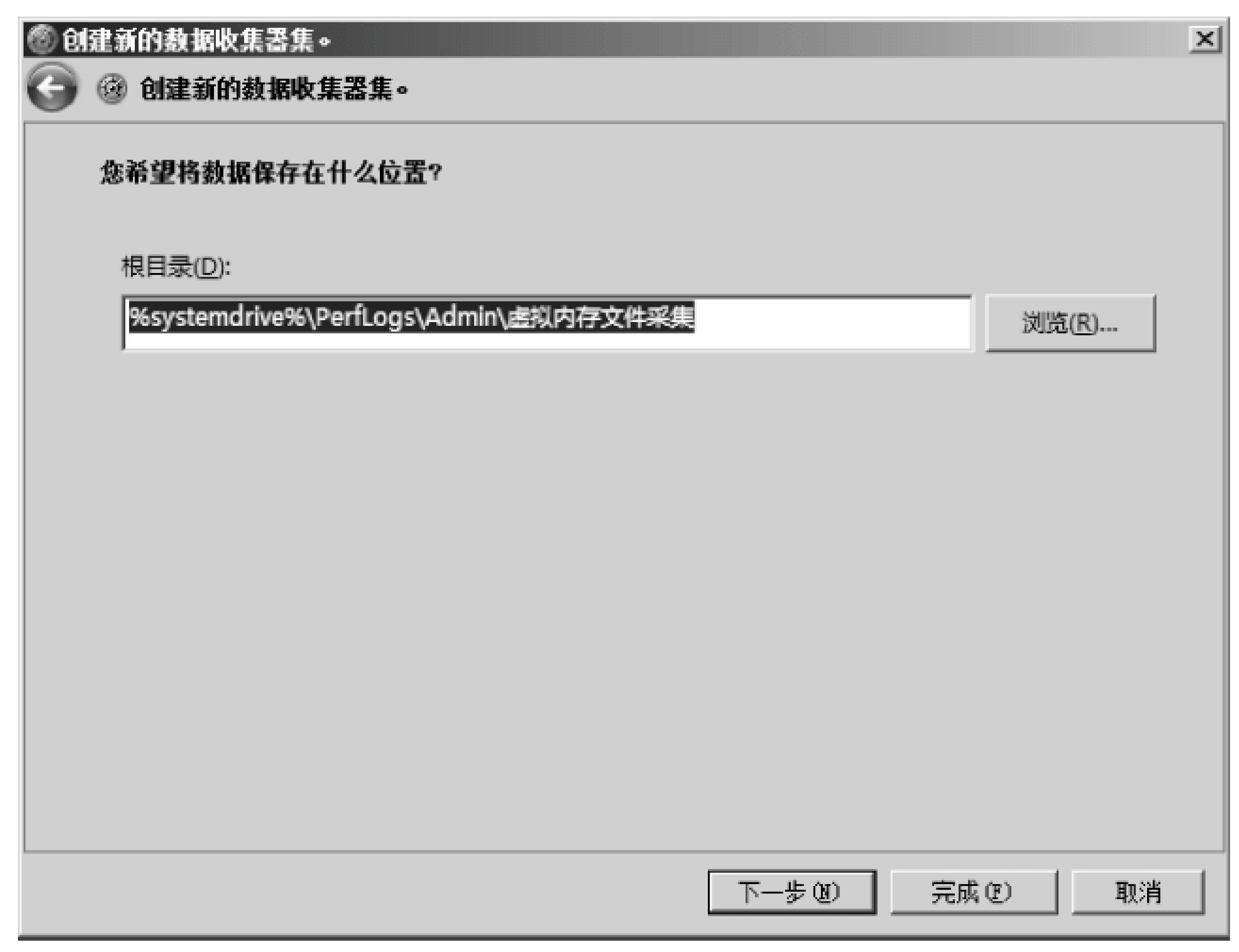


图 3-63　“您希望将数据保存在什么位置”对话框

⑤ 单击“下一步”按钮，显示图 3-64 所示的“是否创建数据收集器集”对话框。本例中选中“保存并关闭”单选按钮，创建新的收集器集但不立即运行该数据收集器集。



图 3-64　“是否创建数据收集器集”对话框

⑥ 单击“完成”按钮，成功创建新的数据收集器集，如图 3-65 所示。

（2）数据采集

用户自定义数据收集器创建完成后，默认并没有启动该收集器。如果要采集数据，需要手动启动该数据收集器。

① 右击需要启动的数据收集器，在快捷菜单中选择“开始”命令，即可开始收集选择的



图 3-65　成功创建性能数据器集

计数器日志。右击目标数据收集器，在快捷菜单中选择“最新的报告”命令，显示图 3-66 所示的窗口，当前系统的状态是“正在收集数据”。



图 3-66　开始收集数据

② 如果需要停止数据收集，右击需要启动的数据收集器，在快捷菜单中选择“停止”命令，即可停止数据收集。采集停止后，右击目标数据收集器，在快捷菜单中选择“最新的报告”命令，显示图 3-67 所示的窗口，显示在监控的时间区域，虚拟内存文件占用的百分比，本例中使用了 50%左右的虚拟内存，说明当前虚拟内存的大小已经远远不能够满足系统的需要，需要管理员根据采集的数据样本，合理地安排计算机资源。



图 3-67 数据采集结果

习题

1. 简述 Windows Server 2008 Server Core 的优缺点。
2. 在“可靠性和性能监视器”中,常用的计数器有哪些?

实验:安装并配置 Windows Server 2008 Server Core

实验目的:

掌握安装 Windows Server 2008 Server Core 的操作,以及掌握 Server Core 的基本配置。

实验内容:

首先安装 Windows Server 2008 Server Core 操作系统,并在安装完成后对 Server Core 进行基本配置。

实验步骤:

(1) 使用 Windows Server 2008 Server Core 安装光盘安装操作系统。

(2) 设置管理员密码。

(3) 设置服务器名称。

(4) 设置 IP 地址。

(5) 设置时区。

(6) 激活服务器。

(7) 启用自动更新。

(8) 启用远程桌面。

(9) 添加角色和功能。

第 4 章 chapter 4

Windows系统安全管理

众所周知，服务器的作用就是为网络提供服务，与客户端计算机相比，服务器端所保存的数据更容易成为病毒、木马和黑客的目标。如果服务器不幸中招，因此而带来的影响将是不可估计的，尤其是处于广域网中的服务器，其被攻击的可能性更大。Windows 系统本身就已经集成了大量的安全工具和策略，可以在很大程度上增加系统的安全性。

4.1 Windows 系统安全管理规划

Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业的运营和发展奠定了坚实的基础。Windows Server 2008 提供了减小内核攻击面的安全创新思路(例如 PatchGuard)，因而使服务器环境更安全、更稳定。通过保护关键服务器服务使之免受文件系统、注册表或网络中异常活动的影响，Windows 服务强化有助于提高系统的安全性。

4.1.1 项目背景

在当前项目网络中，除其中部分服务器使用 Windows Server 2003 操作系统外，其余服务器均使用 Windows Server 2008 操作系统。为了使服务器可以正常地为网络提供服务，必须保证服务器的安全。

4.1.2 项目需求

在网络环境中，服务器的安全主要是提高自身的安全性，从而保证其自身的安全。合理地配置服务器的安全级别、配置强大的安全策略等都是提高服务器安全性的可行方法。另外，对于日常的服务器操作还应该进行相应的记录，如果只是单纯地使用手动记录的方式，显然是不实际的。因此，需要在服务器上使用一种记录机制，记录服务器的所有系统情况。

4.1.3 解决方案

通常情况下，对于 Windows 系统安全管理，可从如下几方面进行操作。

(1) 安全配置向导(SCW)是一个工具，可确定服务器的一个或多个角色所需的最少功能，并且禁用不需要的功能。安全配置向导既可以独立运行，也可以从服务器管理器中运行。用户可以在安全配置向导的指导下，根据服务器选定角色，完成创建、编辑、应用或回滚

安全策略等操作。使用 SCW 创建的安全策略是 XML 文件，服务、网络安全、特定的注册表值、审核策略以及(如果适用)Internet 信息服务(IIS)将被配置到该文件内并被应用。

(2) 设置本地安全策略。顾名思义，本地安全策略是仅用于本地计算机的安全策略。Windows Server 2008 系统的安全机制更为强大，但默认情况下并未配置，因此起不到任何保护作用，必须根据需要启用并配置这些安全策略，以确保系统安全。

(3) 系统日志可以记录下系统所产生的所有行为，并按照某种规范表达出来。使用日志系统所记录的信息为系统进行排错，优化系统的性能，或者根据这些信息调整系统的行为。在安全领域，日志系统的地位更加重要。

4.2　Windows 安全管理工具

凭借超强的功能以及更胜一筹的安全优势，Windows Server 2008 系统吸引了许多网络管理员在不知不觉中前来试用。可是，这并不能说明 Windows Server 2008 系统在安全方面就可以高枕无忧了，因为在不同的使用环境下，Windows Server 2008 系统表现出来的安全防范能力是不一样的，甚至该系统在某些方面没有一点安全抵抗能力，这就需要手动保护 Windows Server 2008 系统的运行安全了。

4.2.1　安全配置向导

安全配置向导可以帮助管理员快速完成创建、编辑、应用和回滚安全策略操作。在 Windows Server 2008 系统中，已经默认集成安全配置向导，用户无须安装即可直接应用。

(1) 依次选择“开始”→“管理工具”→“安全配置向导”命令，打开“欢迎使用安全配置向导”对话框。也可以在“开始”菜单的“开始搜索”文本框中输入 scw. exe 命令，单击“确定”按钮来启动安全配置向导。

(2) 单击“下一步”按钮，显示图 4-1 所示的“配置操作”对话框，这里选中“新建安全策略”单选按钮。



图 4-1　“配置操作”对话框

安全配置向导提供了以下 4 种配置操作。

① 新建安全策略。可以创建用于配置服务、Windows 防火墙、Internet 协议安全(IPsec)设置、审核策略和特定注册表设置的安全策略。安全策略文件是 XML 格式文件，默认保存路径为%systemroot%\security\msscw\Policies。

② 编辑现有安全策略。可以编辑已使用 SCW 创建的安全策略。必须先选中“编辑现有安全策略”单选按钮，才能浏览到要编辑的安全策略文件所在的文件夹。编辑的策略可存储在本地上或网络共享文件夹中。

③ 应用现有安全策略。使用 SCW 创建安全策略后，可将其应用到测试服务器中，或者应用到生产环境中。

提示：在将新创建或新修改的安全策略应用到生产环境之前，首先进行测试，然后将安全策略部署到业务系统中，测试可使新策略在生产环境中导致意外结果的可能性降至最低。

④ 回滚上一次应用的安全策略。如果使用 SCW 应用的安全策略使服务器功能达不到预期的效果，或者导致其他非预期结果，则可以回滚该安全策略，将自动从该服务器删除对应的安全策略。

注意：如果策略是在“本地安全策略”中编辑的，在应用策略后，这些更改就不能回滚到应用前的状态。对于服务和注册表值，回滚过程还原了在配置过程中更改的设置。对于 Windows 防火墙和 IPSec，回滚过程取消当前使用的任何 SCW 策略的分配，并重新分配在上一次应用的策略。

(3) 单击“下一步”按钮，显示图 4-2 所示的“选择服务器”对话框。在“服务器”文本框中，输入需要进行安全配置的 Windows Server 2008 服务器的主机名或 IP 地址。也可以单击“浏览”按钮，选择需要进行安全配置的目标计算机。

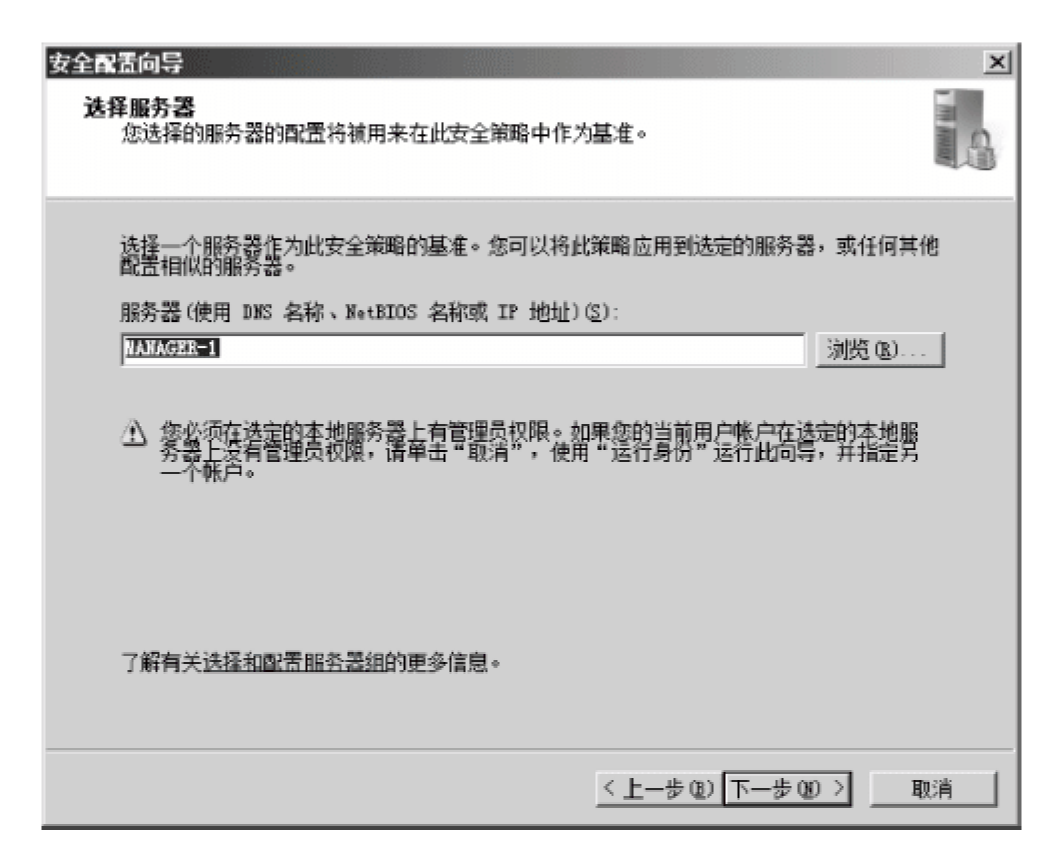


图 4-2 “选择服务器”对话框

(4) 单击“下一步”按钮，开始扫描配置数据库，主要包括已安装或运行的网络服务、IP 地址及子网信息等。扫描完成后显示图 4-3 所示的“正在处理安全配置数据库”对话框。单击“查看配置数据库”按钮，打开“SCW 查看器”窗口，在这里可以查看详细扫描结果。需要注意的是，在此过程中由于 Internet Explorer 7.0 的安全设置，可能会出现安全提示信息，单击“是”按钮跳过即可。

(5) 单击“下一步”按钮，显示“基于角色的服务配置”对话框。安全配置向导可以根据当前服务器提供网络服务的不同，配置相应的安全策略。

(6) 单击“下一步”按钮，显示图 4-4 所示的“选择服务器角色”对话框。系统默认选择“安装的角色”选项，即只设置已安装服务的安全策略。

在“查看”下拉列表框中包括如下 4 种可供选择的角色模式。

① 所有角色：列出所有的 Windows Server 2008 可以使用的角色。

② 安装的角色：列出当前服务器中已经安装的角色，包括没有设置的角色。



图 4-3 “正在处理安全配置数据库”对话框



图 4-4 “选择服务器角色”对话框

③ 未安装的角色：列出当前服务器中没有安装的角色，不包括没有设置的角色。

④ 选定的角色：列出当前服务器中已经选定的角色。

注意：为了保证服务器的安全，仅选择所需要的服务器角色即可。选择多余的服务器角色，会增加 Windows Server 2008 系统的安全隐患。

(7) 单击“下一步”按钮，显示图 4-5 所示的“选择客户端功能”对话框，可以选择当前服务器作为其他服务器的客户端时需要使用的功能，如自动更新客户端等。在“查看”下拉列表框中的选项与“选择服务器角色”中的基本相同，此处不再赘述。

(8) 单击“下一步”按钮，显示图 4-6 所示的“选择管理和其他选项”对话框。在“选择用来管理选定的服务器的选项”列表中，可以选中相应的管理对应的复选框。

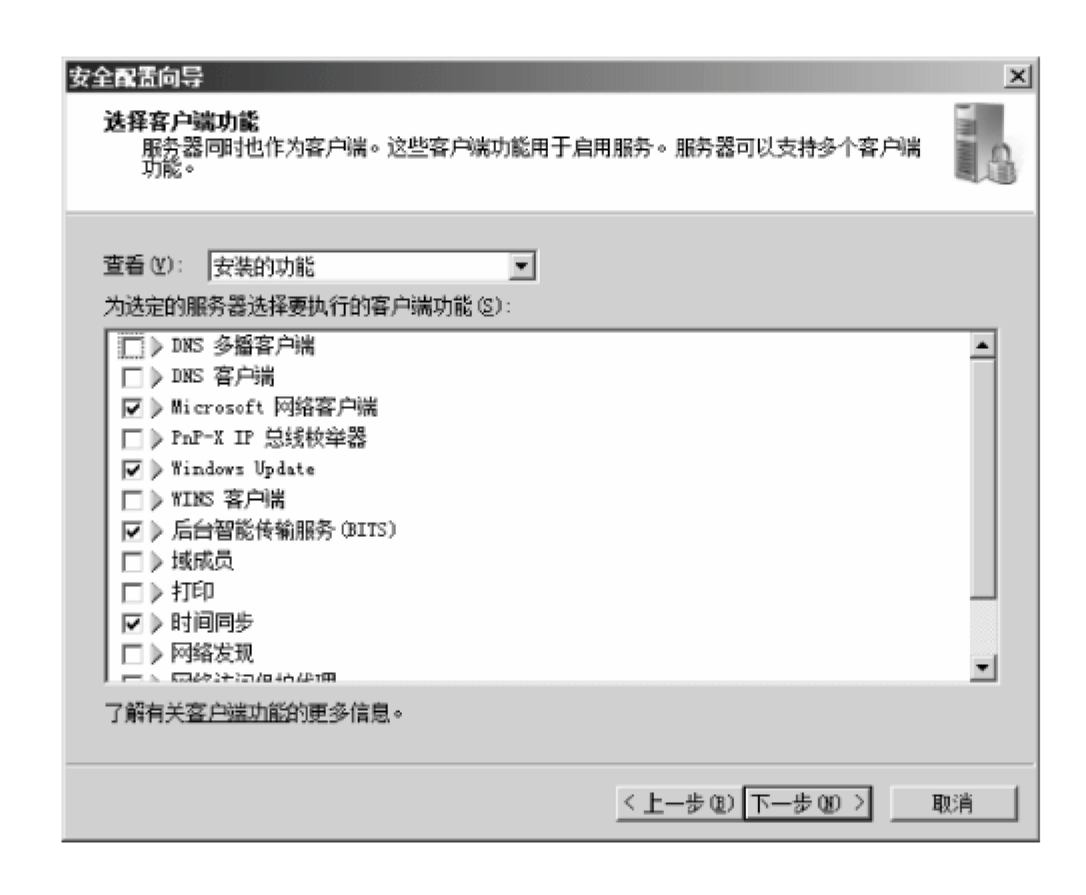



图 4-5 “选择客户端功能”对话框

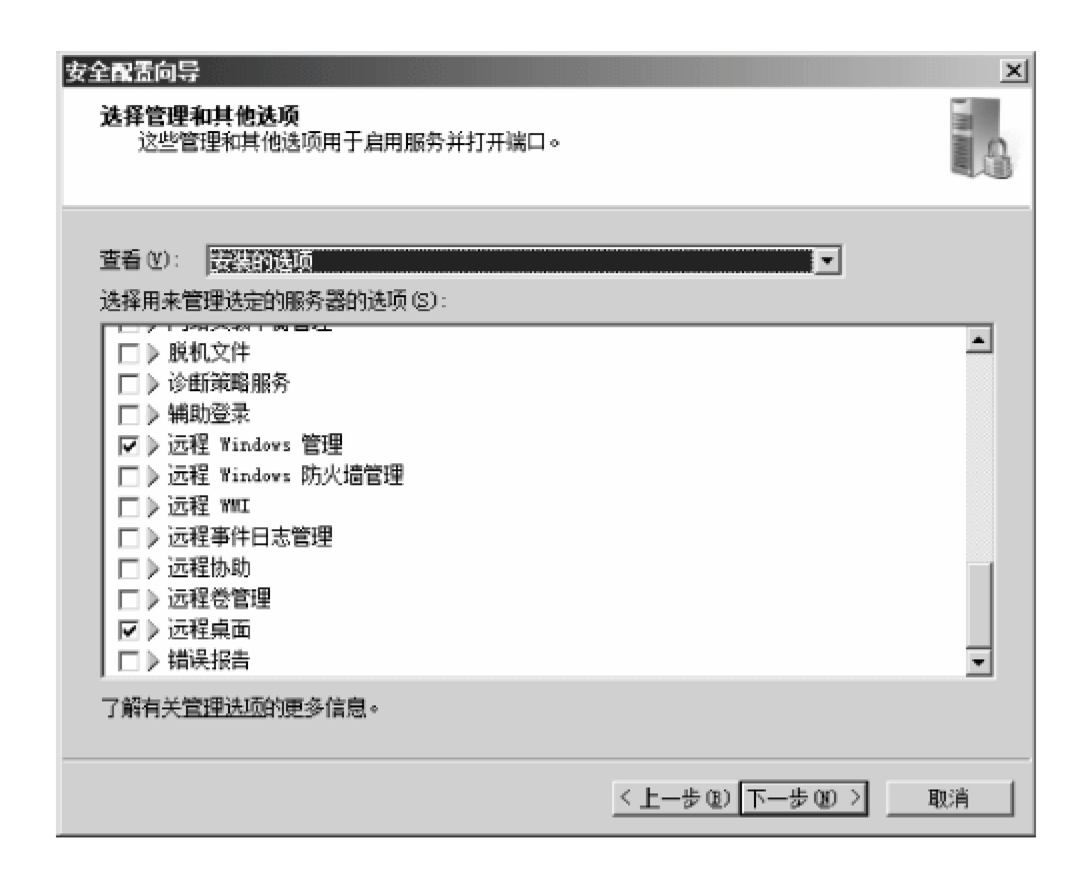


图 4-6 “选择管理和其他选项”对话框

(9) 单击“下一步”按钮，显示图 4-7 所示的“选择其他服务”对话框。其他服务是指当前服务器上已经安装但在安全配置数据库中未显示的服务。如果出现这种情况，安全配置向导将在“选择其他服务”对话框中显示已安装的服务列表。展开相应的服务即可查看其详细运行模式。

(10) 单击“下一步”按钮，显示图 4-8 所示的“处理未指定的服务”对话框。未指定的服务是指安全策略配置向导扫描过程中未能发现的服务，用户可以在这里设置其运行状态，选中“不更改此服务的启动模式”单选按钮即可。

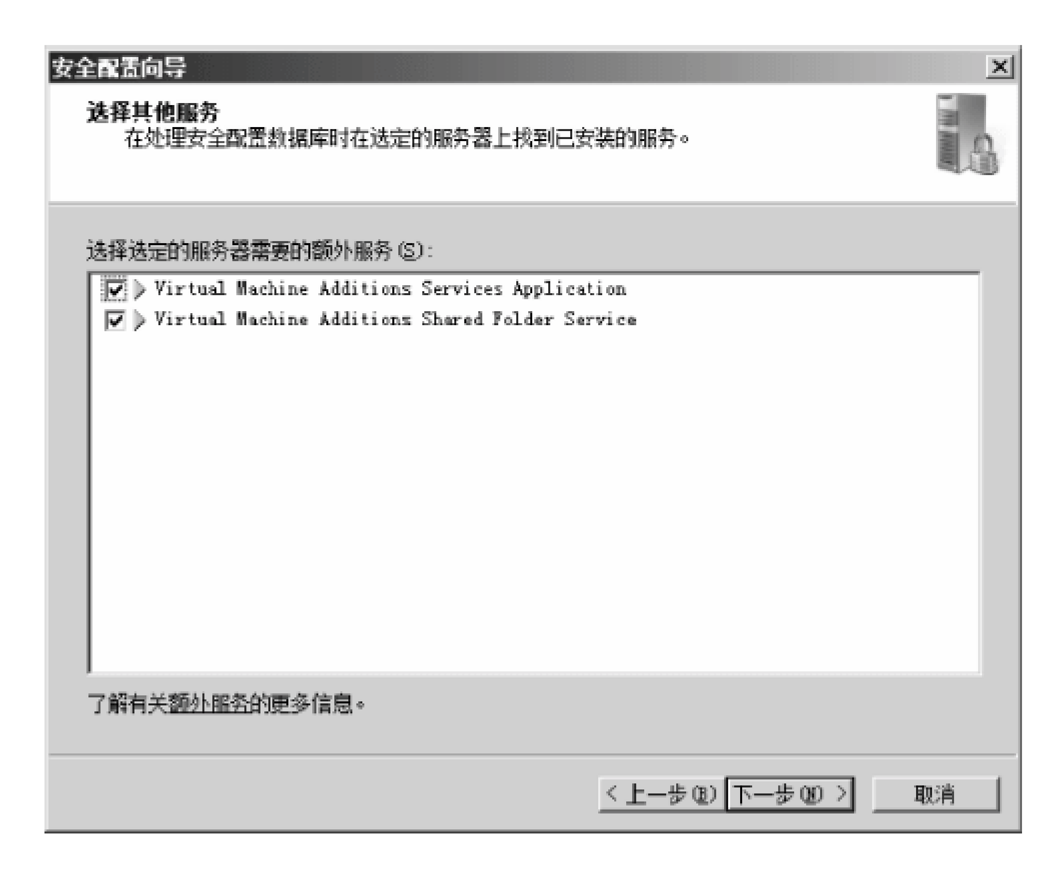


图 4-7 “选择其他服务”对话框

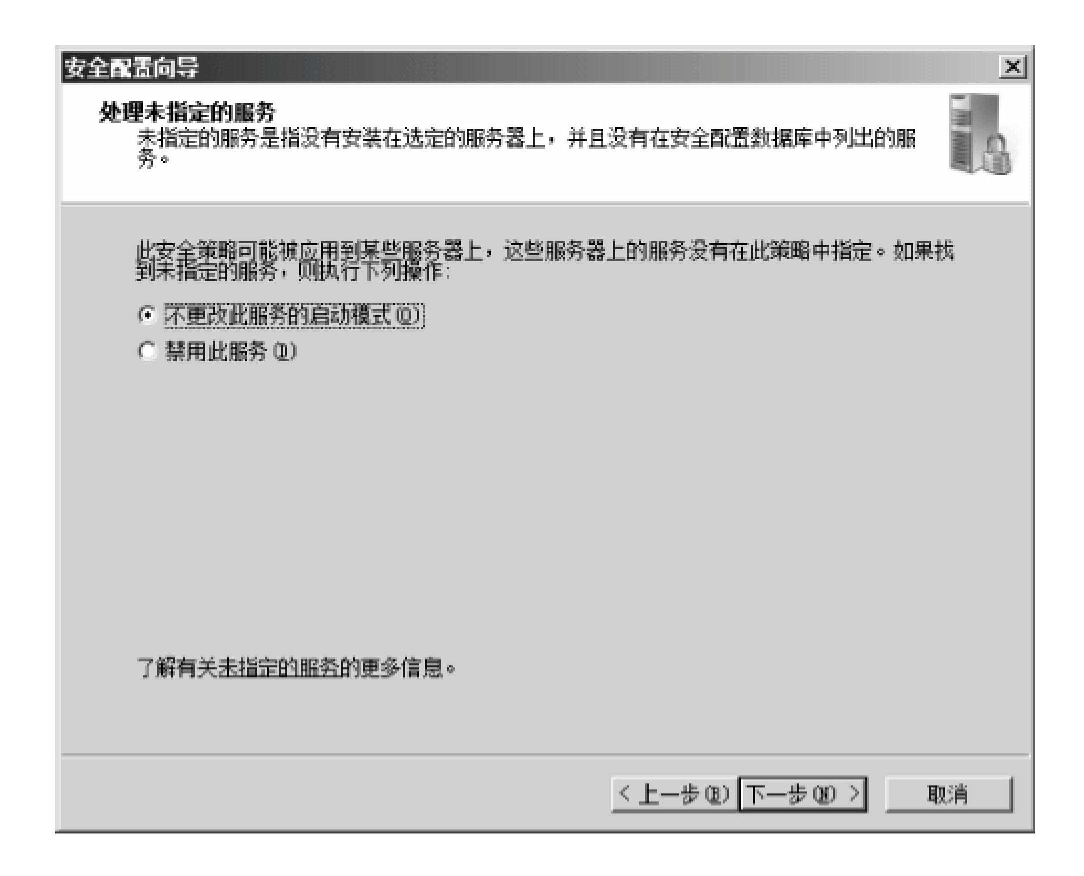


图 4-8 “处理未指定的服务”对话框

两种处理方式的主要区别如下。

① 不更改此服务的启动模式。如果选中此单选按钮，则在应用此安全策略的服务器上启用的未指定服务将保持启用状态，而禁用的那些服务将保持禁用状态。

② 禁用此服务。如果选中此单选按钮，则不在安全配置数据库中的或未安装在选定服务器上的所有服务都将被禁用。

(11) 单击“下一步”按钮，显示图 4-9 所示的“确认服务更改”对话框，系统默认只显示当前服务器上正在运行的服务，服务的启动模式可以是“已禁用”、“手动”或“自动”。在应用

安全策略后，才能对选定服务器做出更改。

（12）单击“下一步”按钮，显示“网络安全”对话框。如果选中“跳过这一部分”复选框，则将跳过“网络安全”配置部分。建议不要跳过此步骤，继续按照如下步骤操作。

（13）单击“下一步”按钮，显示图4-10所示的“网络安全规则”对话框。系统默认在“查看”下拉列表框中显示“所有规则”选项，即该服务器上目前开放的所有端口。也可以在“查看”下拉列表框中选择其他查看方式。单击安全规则前面的三角形按钮，还可以查看其详细信息。

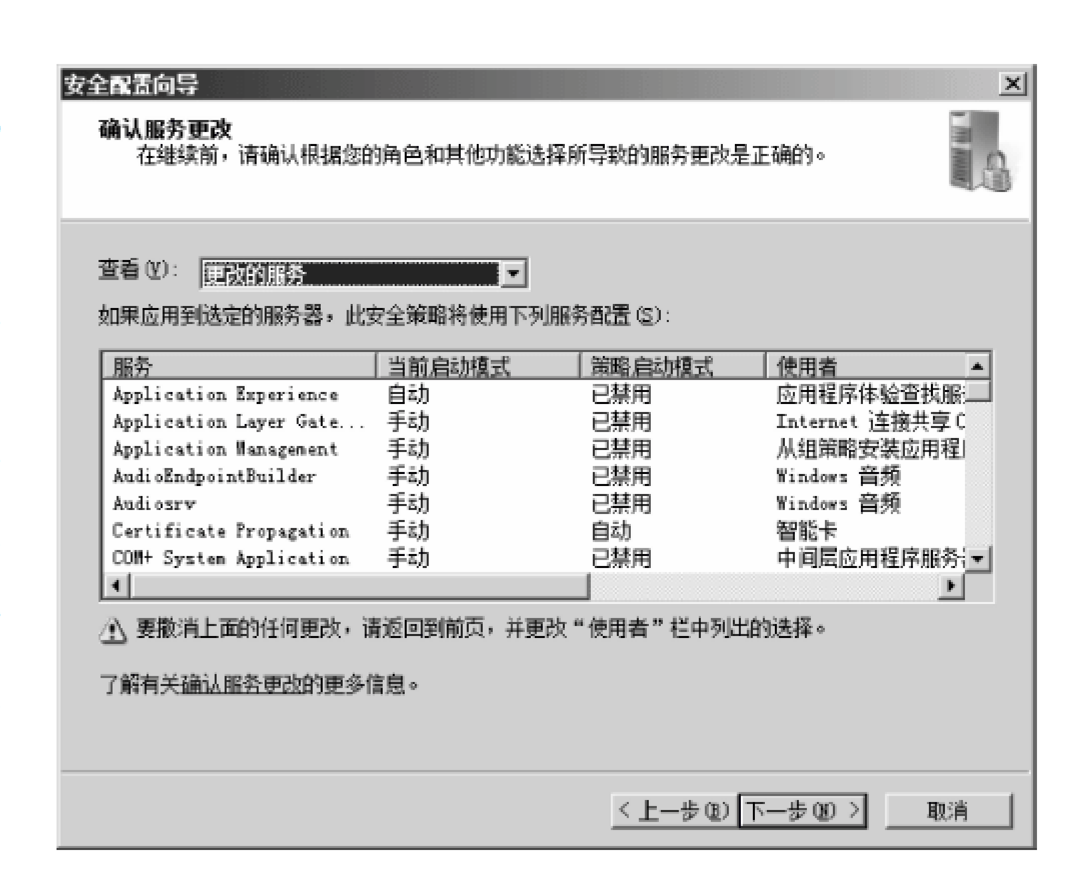


图4-9　“确认服务更改”对话框



图4-10　“网络安全规则”对话框

提示：如果列表中没有列出需要使用的Windows防火墙规则，可以单击“添加”按钮，打开图4-11所示的“添加规则(http)”对话框，将其添加到列表中。在“名称”文本框中，输入防火墙规则的名称，如www，为了便于区分还可以输入相关的描述信息；在“方向”选项区域中，选中“入站”单选按钮；另外，还可以根据需要在“操作”选项区域中选择相应限制连接的方式。



图4-11　“添加规则(http)”对话框

（14）单击“下一步”按钮，显示“注册表设置”对话框。通过该设置可以修改Windows Server 2008服务器注册表中一些特殊键值，从而严格限制用户的访问权限。建议用户不要跳过此步骤。

（15）单击“下一步”按钮，显示图 4-12 所示的“要求 SMB 安全签名”对话框。设置选定的服务器和客户端的通信信息，保持系统默认的全部选择状态即可。

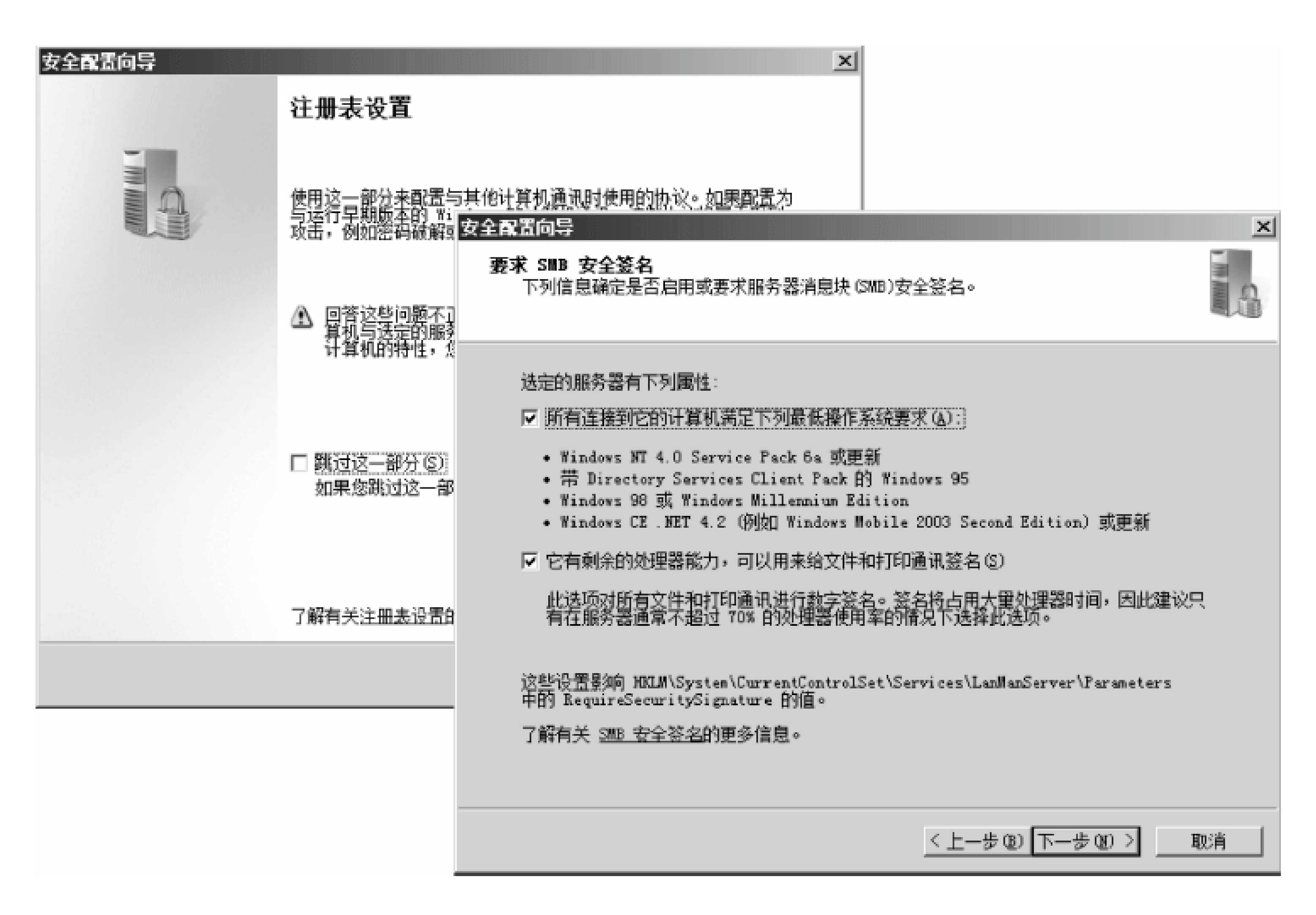


图 4-12 “要求 SMS 安全签名”对话框

（16）单击“下一步”按钮，显示“出站身份验证方法”对话框。选择当前服务器远程连接到其他计算机时使用的身份验证方法，如果是在域网络中进行远程登录，则选中“域账户”复选框即可；如果是工作组环境，建议选中“远程计算机上的本地账户”复选框。

（17）单击“下一步”按钮，显示图 4-13 所示的“出站身份验证使用本地账户”对话框，此对话框中的选项与所选择的出站身份验证方法有关，这里以使用“远程计算机上的本地账户”验证方法为例。通常情况下，保持默认设置即可。



图 4-13 “出站身份验证使用本地账户”对话框

提示：如果不选择任何出站身份验证方法，则单击“下一步”按钮将提示设置“入站身份验证方法”，如图 4-14 所示。入站身份验证方法主要用于当网络用户访问当前计算机时需要使用哪种身份验证方法。如果设置了“出站身份验证方法”则不会出现该对话框。

（18）单击“下一步”按钮，显示图 4-15 所示的“注册表设置摘要”对话框，显示了当前安全策略中所做的注册表安全设置。

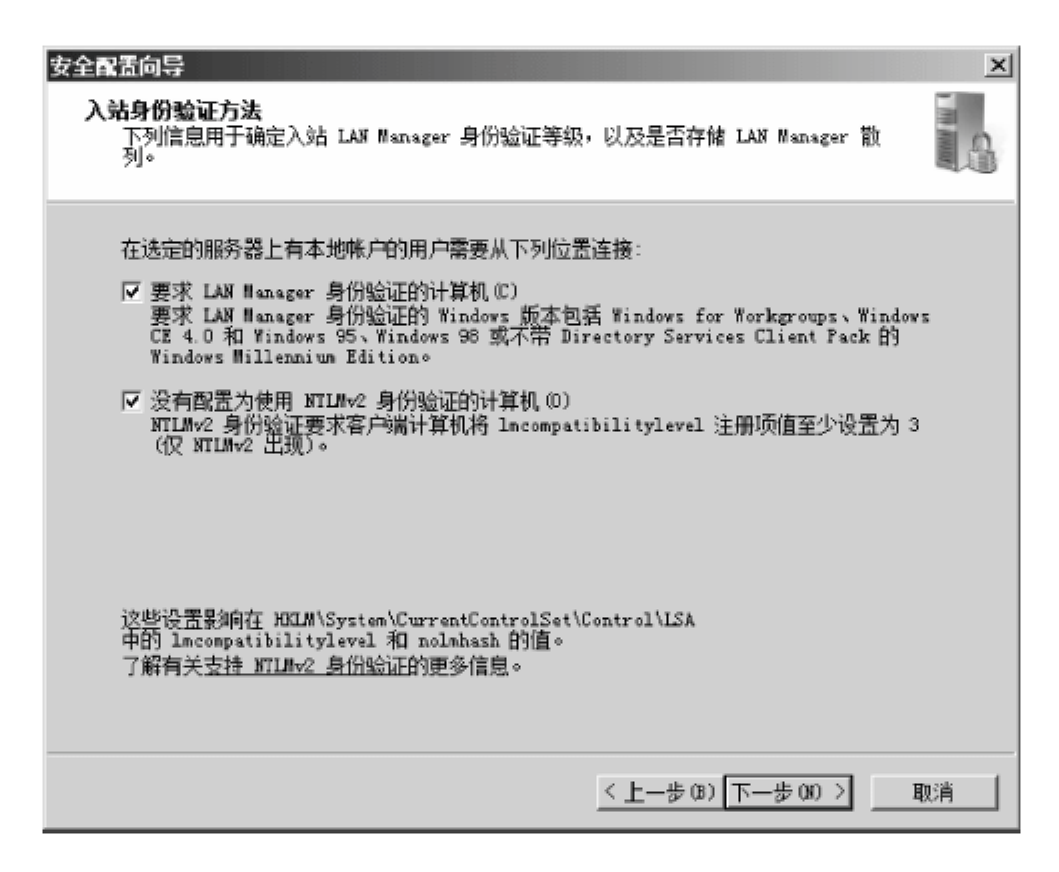



图 4-14 “入站身份验证方法”对话框

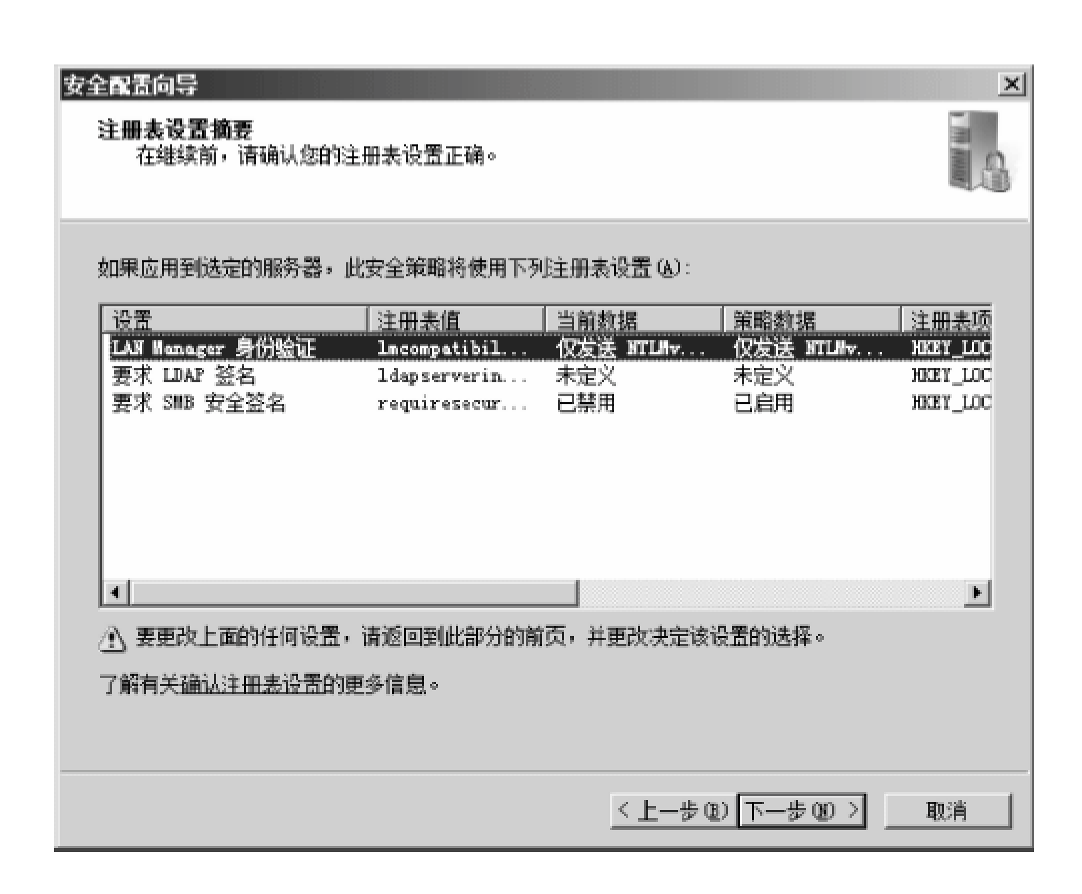


图 4-15 “注册表设置摘要”对话框

（19）单击“下一步”按钮，显示“审核策略”对话框。Windows 审核策略主要用于审核日志记录中的相关内容，并确定受影响的系统对象。安全策略回滚功能是无法回滚安全向导中的审核策略设置的。

（20）单击“下一步”按钮，显示图 4-16 所示的“系统审核策略”对话框。选择需要审核的目标，这里选中“审核成功的操作”单选按钮，即只审核日志记录中操作成功的事件记录。

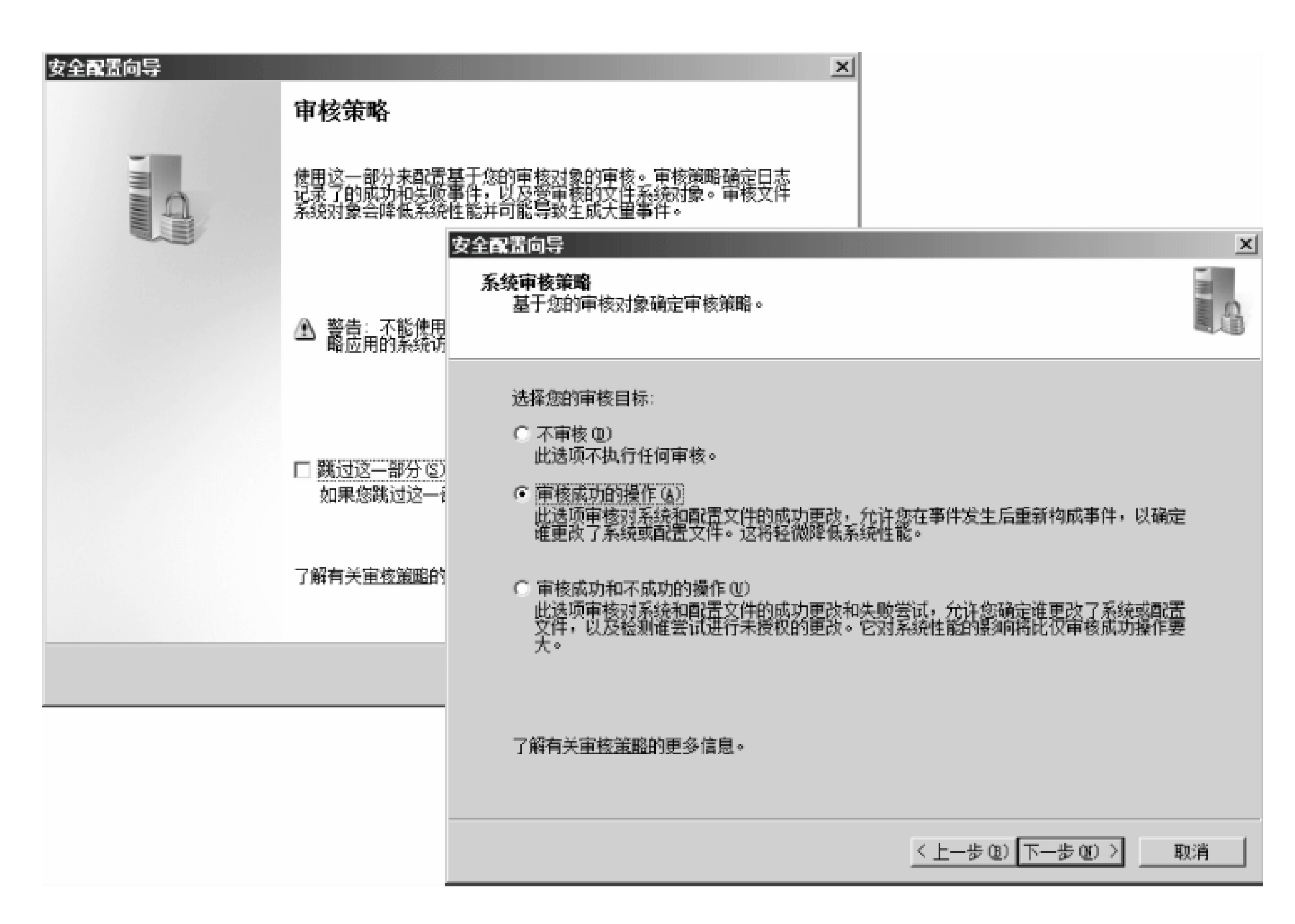


图 4-16 “系统审核策略”对话框

（21）单击“下一步”按钮，显示图4-17所示的“审核策略摘要”对话框。列表中列出了应用策略时，将在选定服务器上应用对审核策略进行的所有更改。在该对话框中显示了每个审核策略设置的当前设置和由策略定义的设置。

（22）单击“下一步”按钮，显示“保存安全策略”对话框。保存完成后，即可将该安全策略应用到当前或其他服务器上。

（23）单击“下一步”按钮，显示图4-18所示的“安全策略文件名”对话框。在保存安全策略文件的路径之后输入安全策略文件名，根据需要输入相关描述信息。

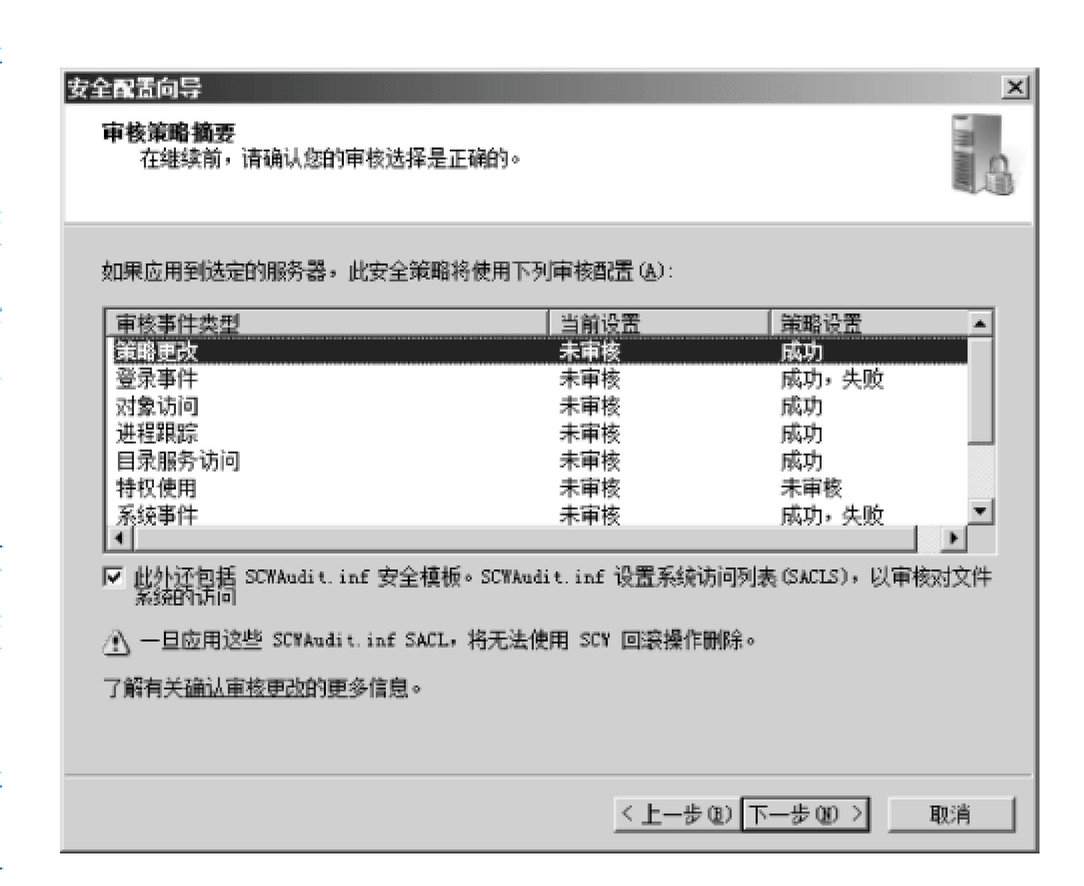


图4-17 “审核策略摘要”对话框



图4-18 “安全策略文件名”对话框

提示：单击“包括安全模板”按钮，还可以向当前安全策略中添加其他安全模板中的安全规则，这些规则将拥有较高的优先级。SCW回滚功能将无法回滚已经应用的策略模板中的规则设置。

（24）单击“下一步”按钮，显示图4-19所示的“应用安全策略”对话框。如果选中“现在应用”单选按钮，则可以将安全策略立即应用到当前服务器；建议选中“稍后应用”单选按钮，使其在测试后再应用到服务器。

（25）单击“下一步”按钮，显示图4-20所示的“正在完成安全配置向导”对话框。单击“完成”按钮，即可完成安全策略的设置。

4.2.2 本地安全策略

打开“运行”对话框，在“打开”文本框中输入gpedit.msc命令，单击“确定”按钮，即可打

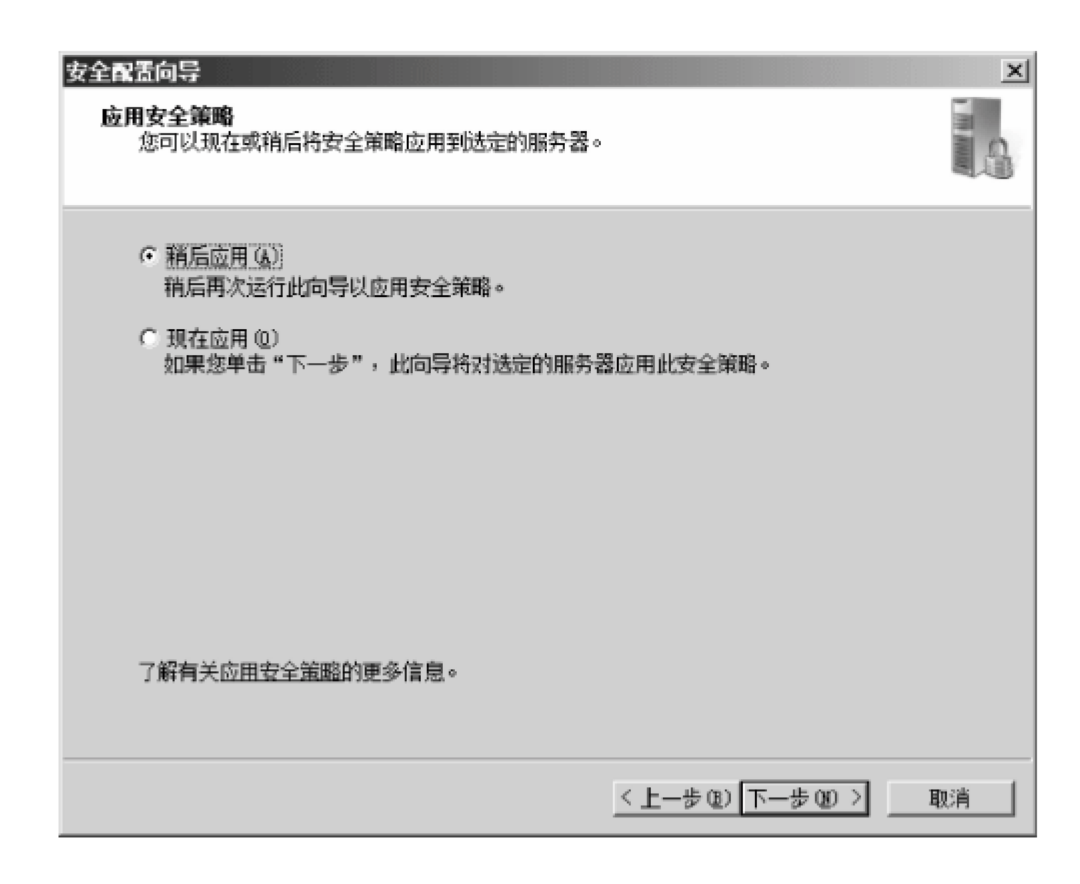


图 4-19 "应用安全策略"对话框



图 4-20 "正在完成安全配置向导"对话框

开"本地组策略编辑器"窗口。依次展开"本地计算机 策略"→"计算机配置"→"Windows 设置"→"安全设置"目录，即可开始配置相应策略，如图 4-21 所示。



图 4-21 "本地组策略编辑器"窗口

1. 密码策略

在 Windows Server 2008 系统中，默认已经为所有用户账户启用了密码策略，其中策略细节如下。

① 密码必须符合复杂性要求。

② 最短密码长度最小值。

③ 密码最短使用期限。

④ 密码最长使用期限。

⑤ 强制密码历史。

⑥ 用可还原的加密来储存密码。

小知识：密码策略是账户策略的一部分，账户策略主要用于限制用户账户的交互方式，其中包括密码策略和账户锁定策略，这些设置同时适用于独立服务器和域环境。密码策略

用于保护域或本地用户账户的密码安全,设定密码规则等;账户锁定策略用于保护域或本地用户账户的登录安全,确定某个账户被锁定在系统之外的情况和时间长短。

(1) 在"安全设置"选项下依次展开"账户策略"→"密码策略"目录,在右侧窗口中双击"密码必须符合复杂性要求"策略,显示图 4-22 所示的对话框,选中"已启用"单选按钮,即可启用该策略,最后单击"确定"按钮保存。此安全设置确定用户账户密码是否必须符合复杂性要求,如果启用此策略,密码必须符合下列最低要求。

① 不能包含用户的账户名,不能包含用户姓名中超过两个连续字符的部分。

② 至少有 6 个字符长。

③ 至少包含以下 4 类字符中的 3 类字符。

- 英文大写字母(A～Z)。
- 英文小写字母(a～z)。
- 10 个基本数字(0～9)。
- 非字母字符(例如,!、$、#、%)。

④ 在更改或创建密码时执行复杂性要求。

(2) 双击"密码长度最小值"策略,显示图 4-23 所示的对话框,在"密码必须至少是"文本框中设置密码的最小长度,例如 10。最后单击"确定"按钮保存。此安全设置确定用户账户密码包含的最少字符数,可选值范围为 1～14,如果直接设置为 0,则表示允许不设置密码。在 Windows Server 2008 系统中,独立服务器的默认值为 0,而域控制器默认值为 7。

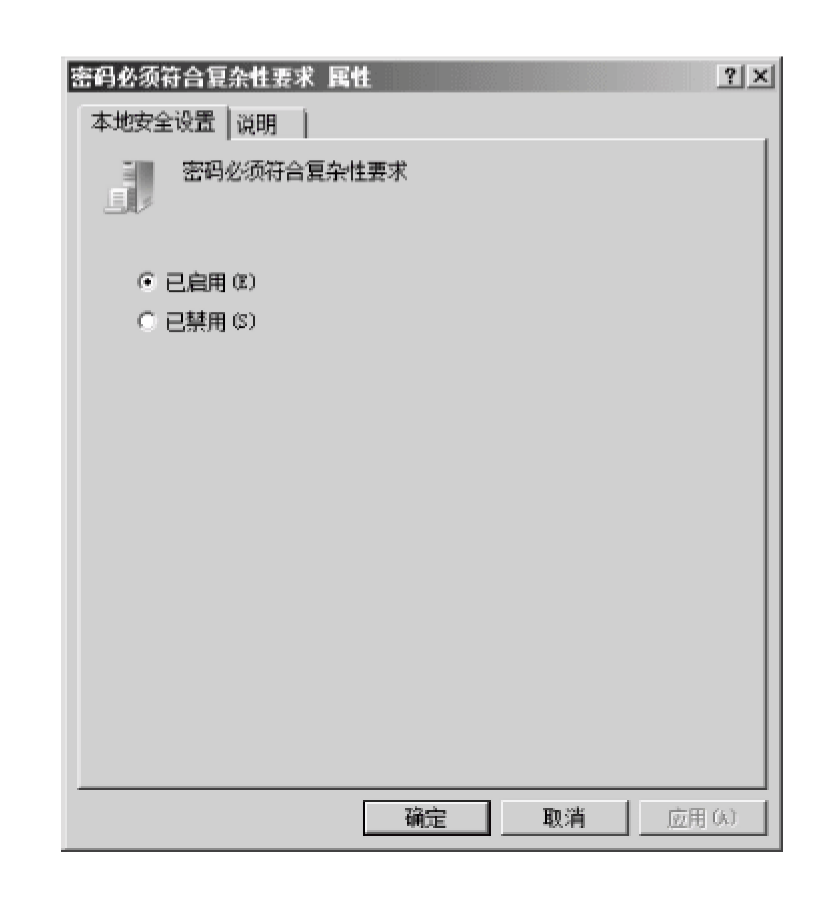


图 4-22 "密码必须符合复杂性要求 属性"对话框

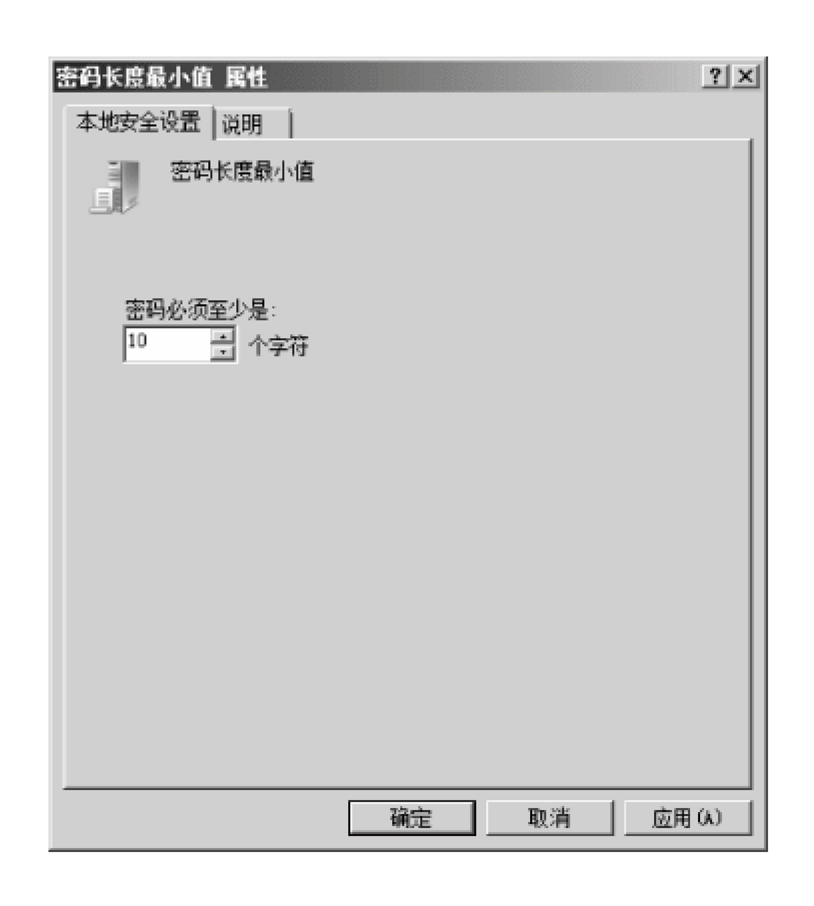
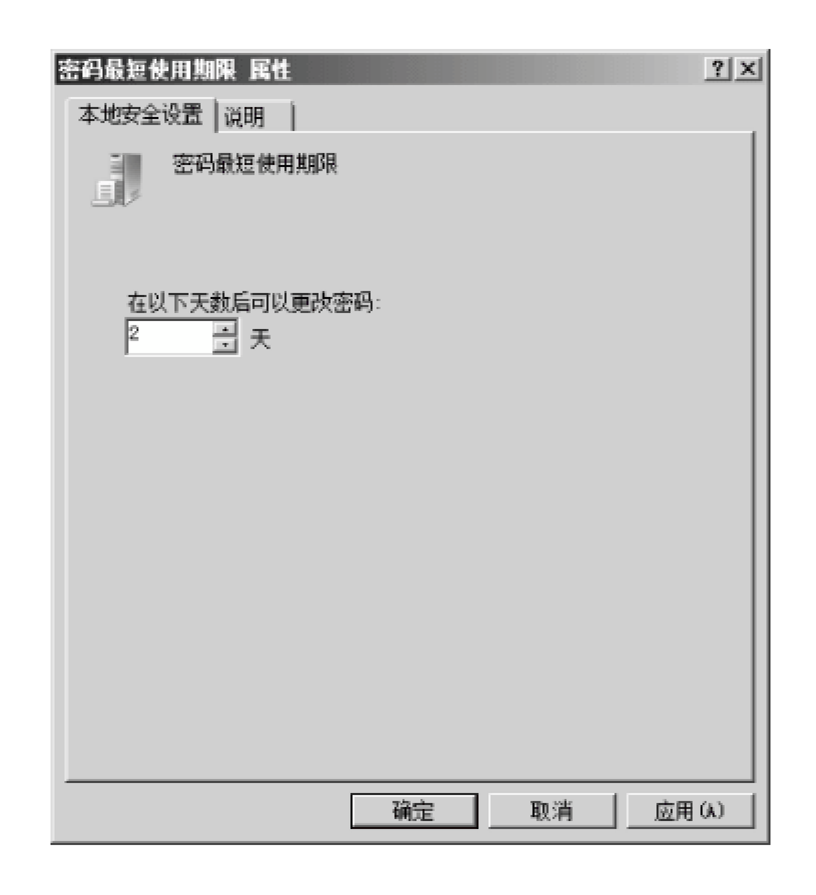


图 4-23 "密码长度最小值 属性"对话框

(3) 双击"密码最短使用期限"策略,显示图 4-24 所示的对话框,Windows Server 2008 系统的独立服务器默认值为 0,域控制器默认值为 1 天。在"在以下天数后可以更改密码"文本框中,输入相应天数(如 2 天),单击"确定"按钮保存即可。

(4) 双击"密码最长使用期限"策略,显示图 4-25 所示的对话框,系统默认"密码过期时间"为 42 天,可选值范围为 1～999 天,如果直接设置为 0,则表示密码永不过期。Windows Server 2008 系统的默认值为 42 天。

注意:安全最佳操作是将密码设置为 30～90 天后过期,具体取决于系统环境及需求。这样,攻击者用来破解用户密码以及访问网络资源的时间将受到限制。





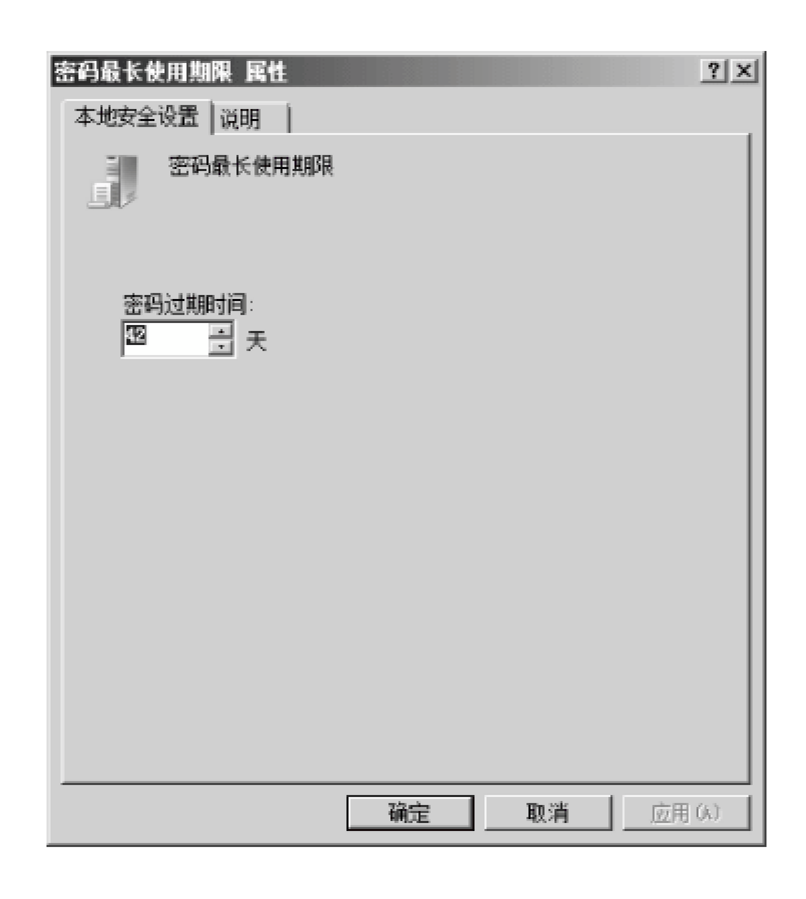
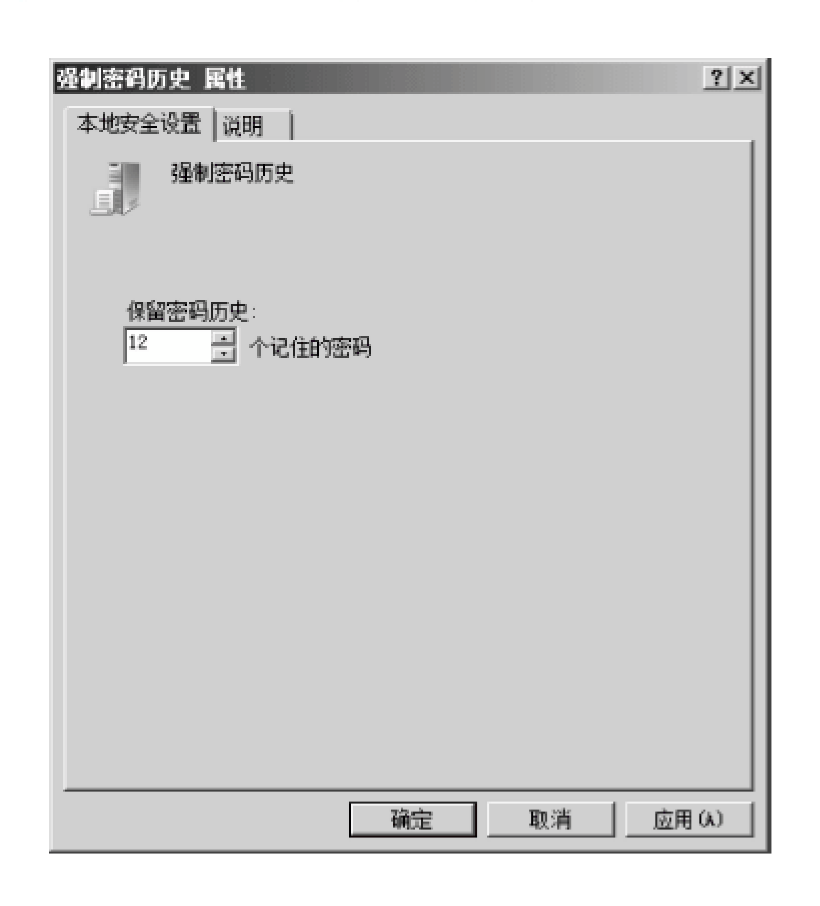


图 4-24 “密码最短使用期限 属性”对话框　　图 4-25 “密码最长使用期限 属性”对话框

(5) 双击“强制密码历史”策略，显示图 4-26 所示的对话框，该策略用于限制用户更改账户密码之前不得使用的旧密码个数，有效范围为 0～24，例如，可以设置为 12，则用户不能重复使用在此之前用过的 12 个历史密码。在 Windows Server 2008 系统中，独立服务器上默认值为 0，域控制器上默认值为 24。

(6) 双击“用可还原的加密来储存密码”策略，显示图 4-27 所示的对话框，该安全设置确定操作系统是否使用可还原的加密来储存密码。选中“已启用”单选按钮，表示允许使用可还原的加密储存密码。单击“确定”按钮保存设置。使用此安全设置，确定操作系统是否使用可还原的加密来储存密码，此策略还可以为某些应用程序提供支持。使用可还原的加密储存密码与储存纯文本密码，在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此策略。



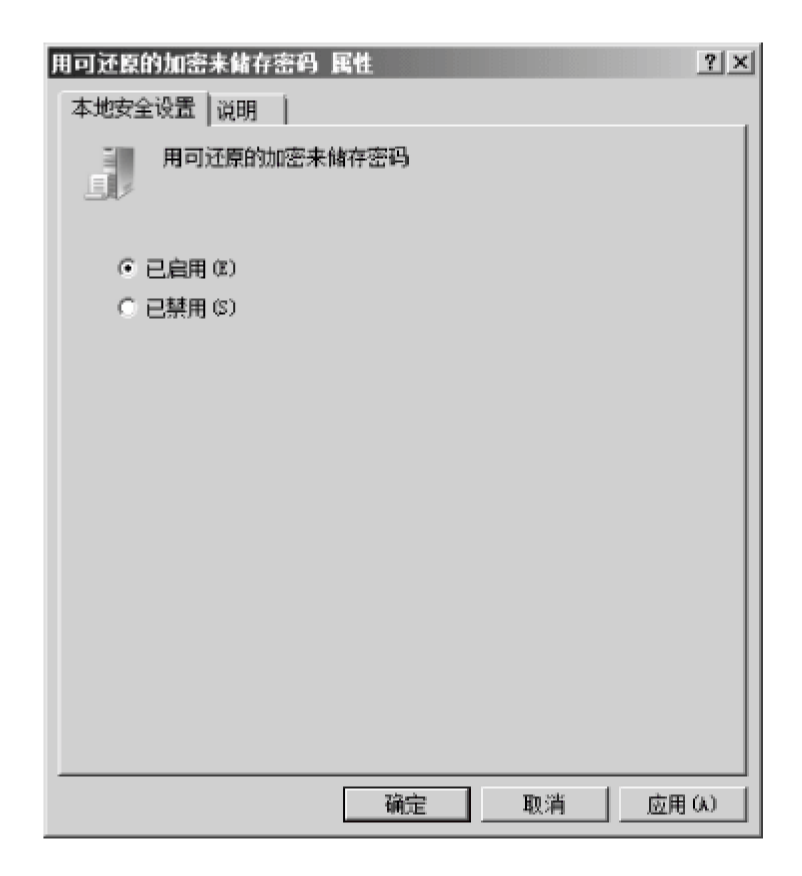


图 4-26 “强制密码历史 属性”对话框　　图 4-27 “用可还原的加密来储存密码 属性”对话框

推荐的密码策略如下。

(1) “密码必须符合复杂性要求”——已启用，必须启用。

(2) “密码长度最小值”——8 个字符或者更高。

提示：密码复杂性是指密码中必须包含字母、数字、特殊符号等内容。对安全性要求比

较高的地方，推荐使用超过12位以上的密码长度。密码应该经常性更换，特别在有管理员以外的人知道时。系统管理员Administrator密码建议仅有管理员知道，且是足够强壮的密码，并且修改默认的用户名。

2. 账户锁定策略

锁定账户可以有效防止入侵者无休止地尝试登录，账户锁定策略主要用于确定某个用户账户被锁定条件和时间长短，具体策略如下。

① 复位账户锁定计数器。

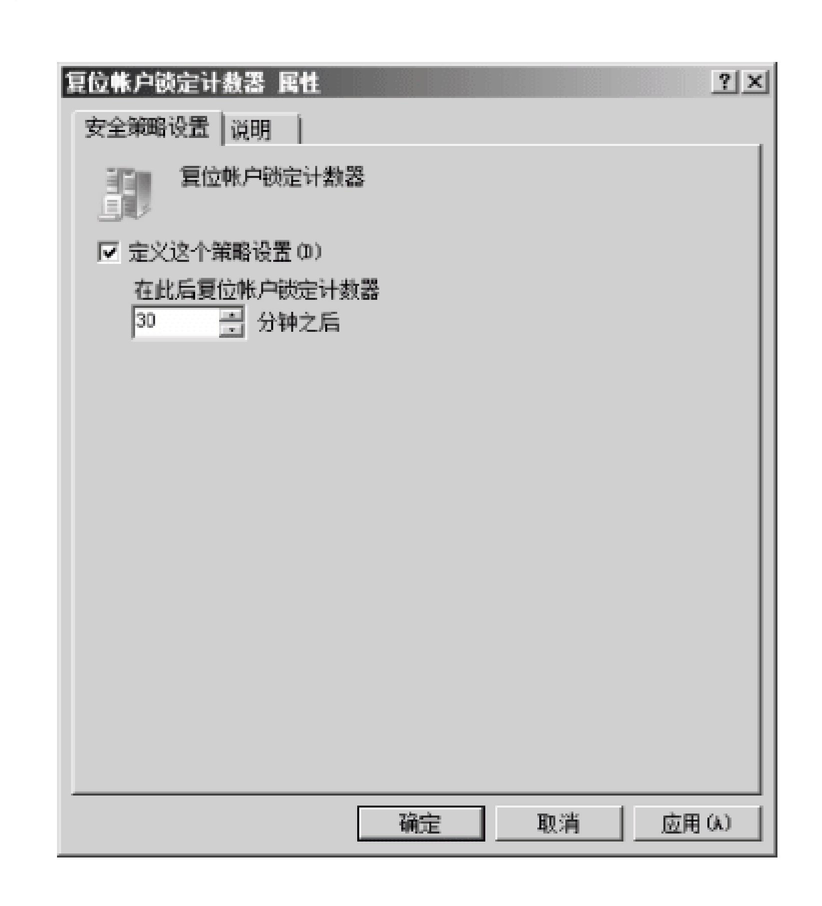
② 账户锁定时间。

③ 账户锁定阈值。

提示：默认情况下，Windows Server 2008系统的独立服务器，并未配置“复位账户锁定计数器”策略和“账户锁定时间”策略，所以管理员账户无法对普通账户实施锁定。

(1) 在Windows Server 2008域控制器上，双击“复位账户锁定计数器”策略，显示图4-28所示的对话框，选中“定义这个策略设置”复选框，并在“在此后复位账户锁定计数器”文本框中输入适当的时间值，默认为30分钟，即账户被锁定30分钟后，才允许再次尝试登录。如果定义了账户锁定阈值，此重置时间必须小于或等于账户锁定时间。

(2) 在Windows Server 2008域控制器上，双击“账户锁定时间”策略，显示图4-29所示的对话框，选中“定义这个策略设置”复选框，并在“账户锁定时间”文本框中输入适当的时间值，默认锁定时间为30分钟。需要注意的是，只有在指定了账户锁定阈值时，此策略设置才有意义。



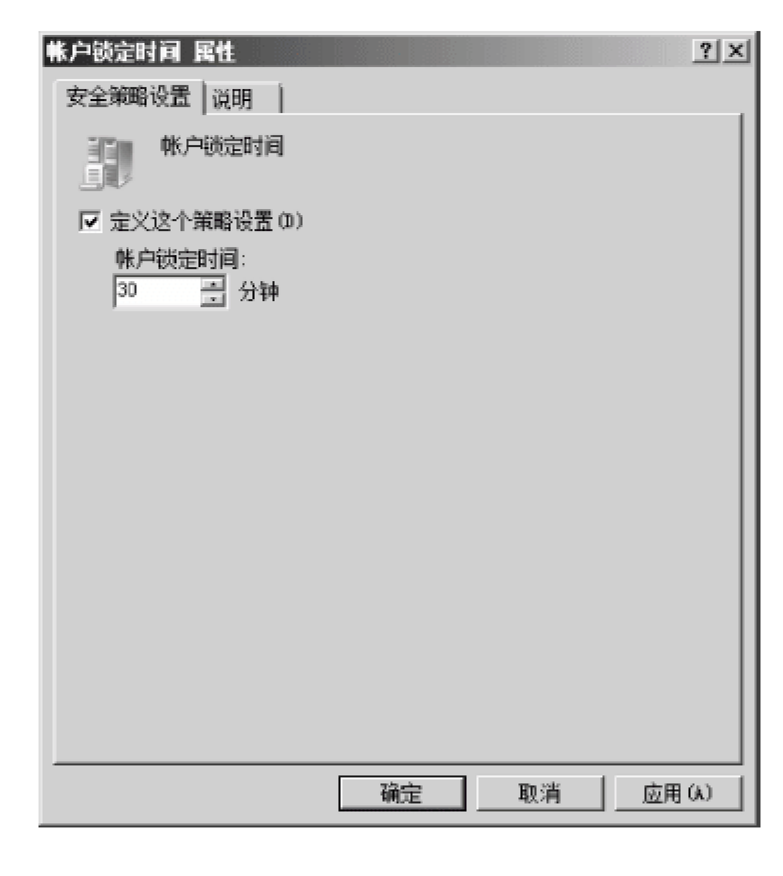



图4-28 “复位账户锁定计数器 属性”对话框

图4-29 “账户锁定时间 属性”对话框

(3) 在Windows Server 2008域控制器或独立服务器上，双击“账户锁定阈值”策略，显示图4-30所示的对话框即启用该策略。Windows Server 2008独立服务器的默认值为0，即永不锁定账户，域控制器默认是未配置的。当使用Ctrl+Alt+Del键或密码保护的屏幕保护程序锁定计算机时，也将记录尝试失败。

推荐的账户锁定策略如下。

(1) “账户锁定阀值”——3次(或者略高)无效登录。

(2) “账户锁定时间”——30分钟(默认，可根据实际需要更改)。

(3) “复位账户锁定计数器”——30 分钟(默认,可根据实际需要更改)之后。

3. Kerberos 策略(Windows 域安全)

Kerberos 策略是适用于域用户账户的安全策略,独立服务器系统无此策略,主要用于确定与 Kerberos 相关的设置,例如票证的有效期限和强制执行。Kerberos 策略不存在于本地计算机策略中。Kerberos 策略中包含如下设置。

① 服务票证最长寿命。

② 计算机时钟同步的最大容差。

③ 强制用户登录限制。

④ 用户票证续订最长寿命。

⑤ 用户票证最长寿命。

(1) 双击“服务票证最长寿命”策略,显示图 4-31 所示的“服务票证最长寿命 属性”对话框,选中“定义这个策略设置”复选框,并在“票证过期时间”文本框中设置适当值即可,默认为 600 分钟。该策略用来设置确定使用所授予的会话票证可访问特定服务的最长时间(以分钟为单位)。该设置必须大于 10 分钟,并且小于或等于用户票证最长寿命设置。

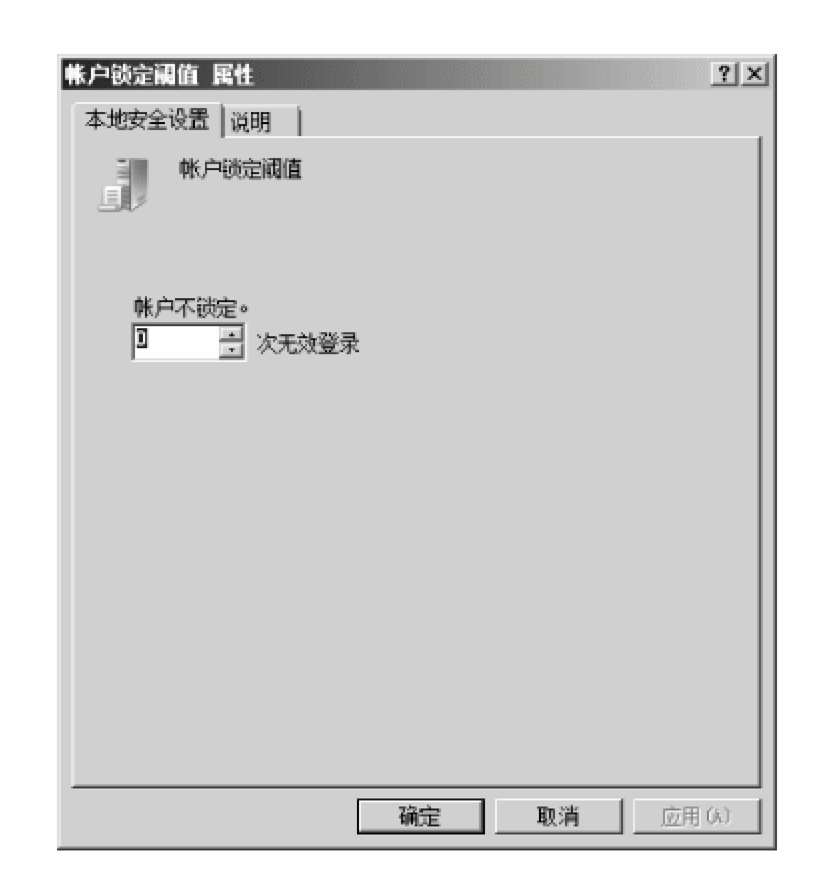



图 4-30 “账户锁定阈值 属性”对话框

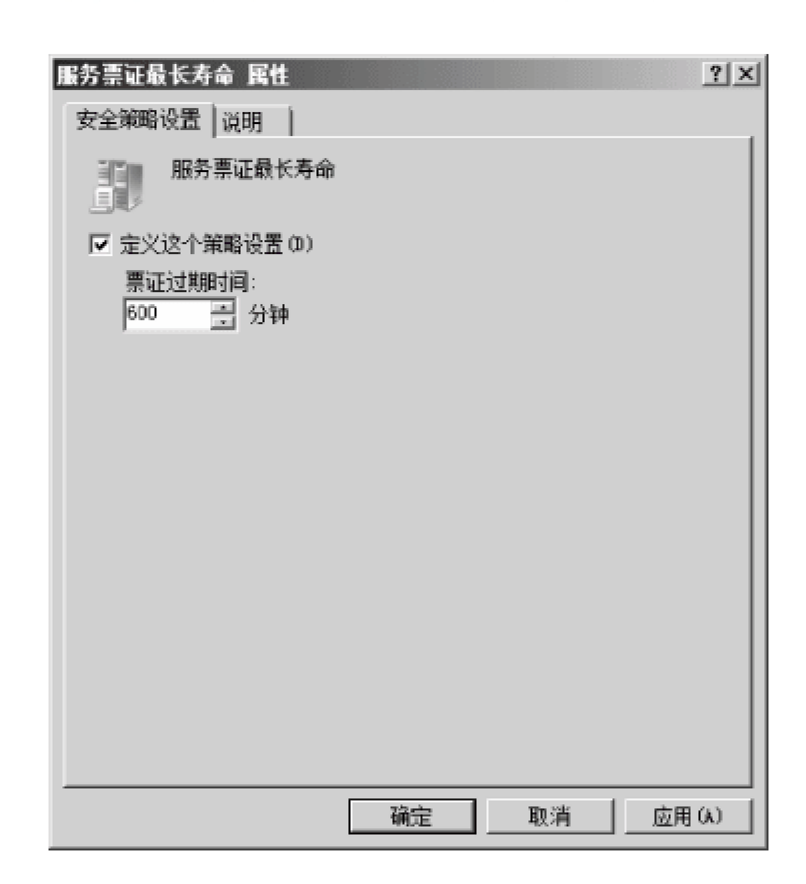


图 4-31 “服务票证最长寿命 属性”对话框

如果客户端请求服务器连接时出示的会话票证已过期,服务器将返回错误消息。客户端必须从 Kerberos V5 密钥分发中心(KDC)请求新的会话票证,然而一旦连接通过了身份验证,该会话票证是否仍然有效就无关紧要了。会话票证仅用于验证和服务器的新建连接。如果用于验证连接的会话票证在连接时过期,则当前的操作不会中断。

(2) 双击“计算机时钟同步的最大容差”策略,显示图 4-32 所示的“计算机时钟同步的最大容差 属性”对话框,选中“定义这个策略设置”复选框,并在“最大容差”文本框中设置适当值即可,默认为 5 分钟。该策略用来设置确定 Kerberos V5 所允许的客户端时钟和提供 Kerberos 身份验证的 Windows Server 2008 域控制器上的时间的最大差值。

提示:该设置并不是永久性的。如果配置该设置后重新启动计算机,那么该设置将被还原为默认值。

(3) 双击“强制用户登录限制”策略,显示图 4-33 所示的“强制用户登录限制 属性”对话框,选中“定义这个策略设置”复选框,并选中“已启用”单选按钮,即可启用该策略。该策略用来设置确定 Kerberos V5 密钥分发中心是否要根据用户账户的用户权限,验证每一个会

话票证请求。验证每一个会话票证请求是可选的,因为额外的步骤需要花费时间,并可能降低服务的网络访问速度。

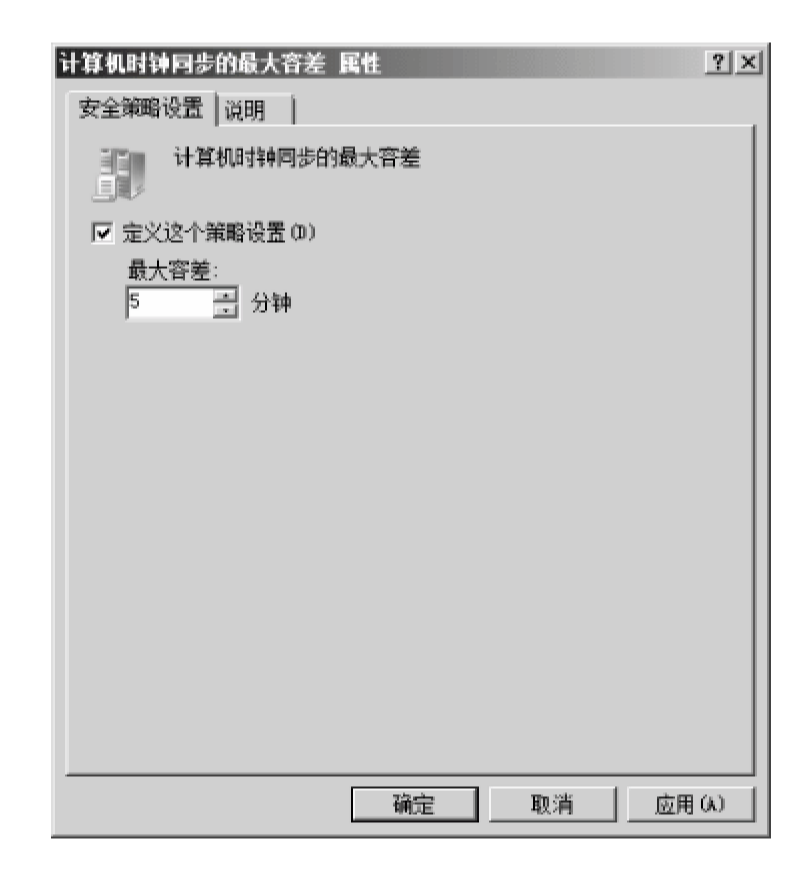


图 4-32 “计算机时钟同步的最大容差 属性”对话框

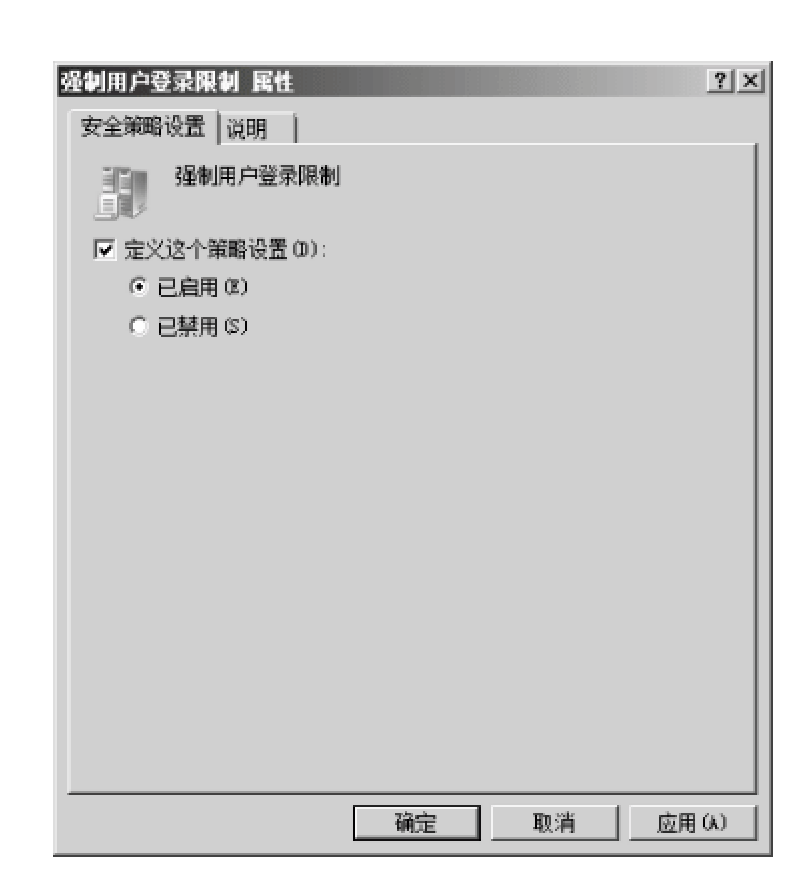


图 4-33 “强制用户登录限制 属性”对话框

(4) 双击“用户票证续订最长寿命”策略,显示图 4-34 所示的“用户票证续订最长寿命 属性”对话框,选中“定义这个策略设置”复选框,并在“票证续订过期时间”文本框中设置适当值即可,默认为 10 天。

(5) 双击“用户票证最长寿命”策略,显示图 4-35 所示的“用户票证最长寿命 属性”对话框,选中“定义这个策略设置”复选框,并在“票证过期时间”文本框中设置适当值即可,默认为 7 个小时。该策略用来设置确定用户票证授予票证(TGT)的最长使用时间,用户 TGT 期满后,必须请求新的或“续订”现有的用户票证。

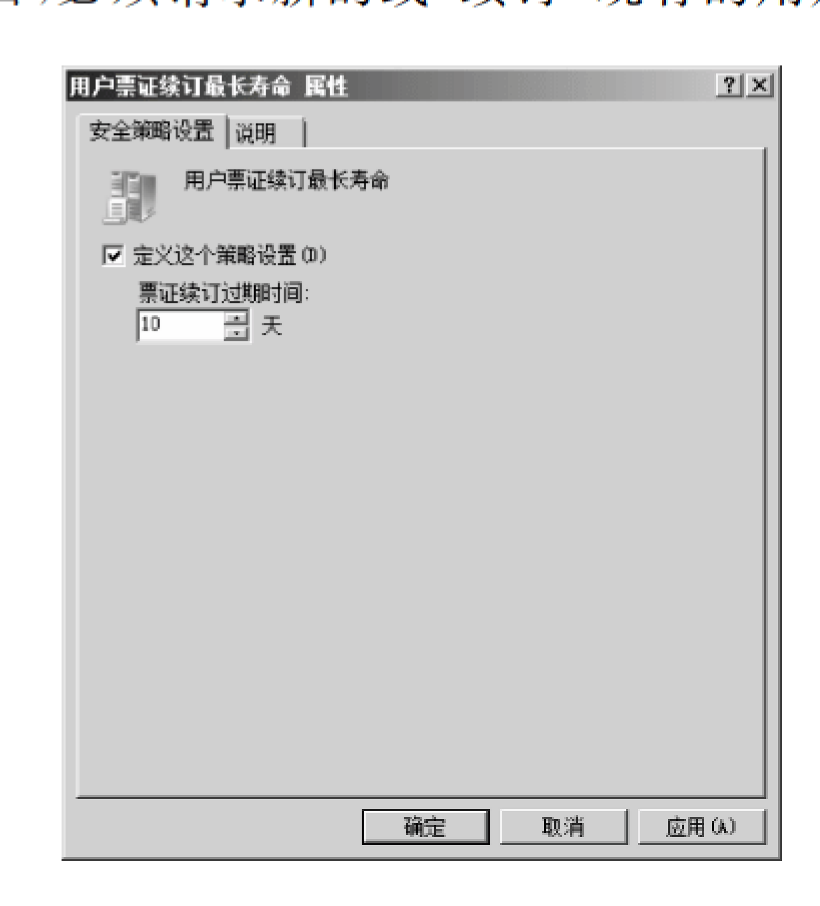



图 4-34 “用户票证续订最长寿命 属性”对话框

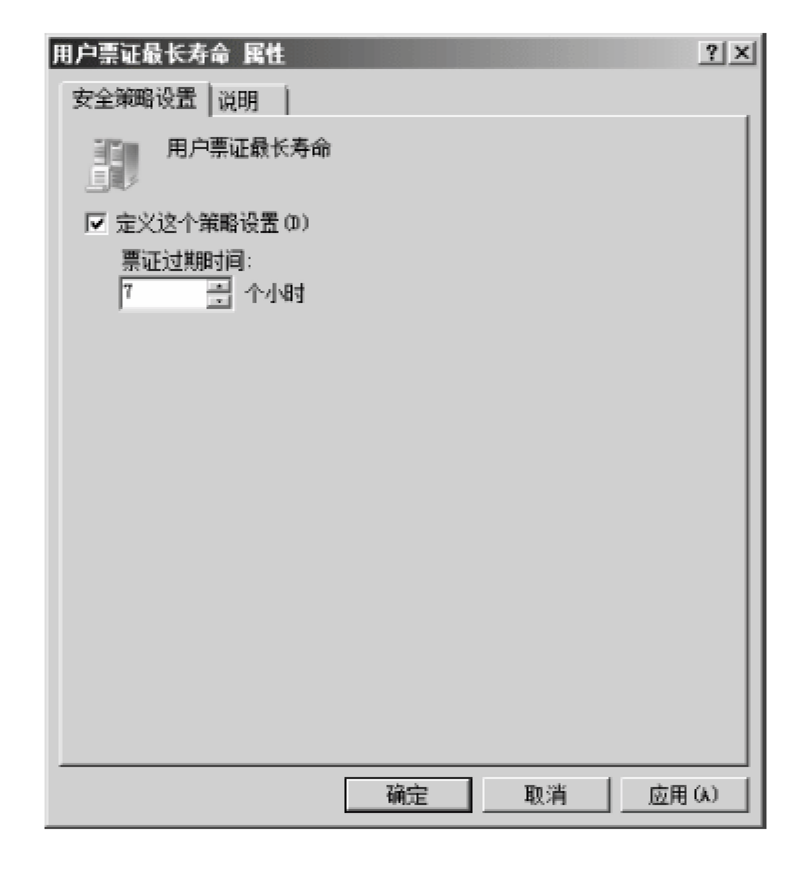


图 4-35 “用户票证最长寿命 属性”对话框

4. 审核策略更改

审核是 Windows Server 2008 本地安全策略中的一部分,是维护系统安全性的工具。通过设置审核策略,管理员可以确定是否将安全事件记录到计算机上的安全日志,同时也确定是否记录登录成功或登录失败,或两者都记录。

(1) 在“本地组策略编辑器”窗口中,依次展开“计算机配置”→“Windows 设置”→“安全

设置”→“本地策略”→“审核策略”目录，在右侧显示审核策略中所包含的策略，如图 4-36 所示。执行审核策略前，必须决定要审核的事件类别。为事件类别选择的审核设置将定义审核策略。

(2) 双击“审核策略更改”策略，显示图 4-37 所示的“审核策略更改 属性”对话框。默认情况下，该策略的值为“无审核”，根据不同的要求选中“成功”或“失败”复选框即可，可同时选中。





图 4-36 审核策略

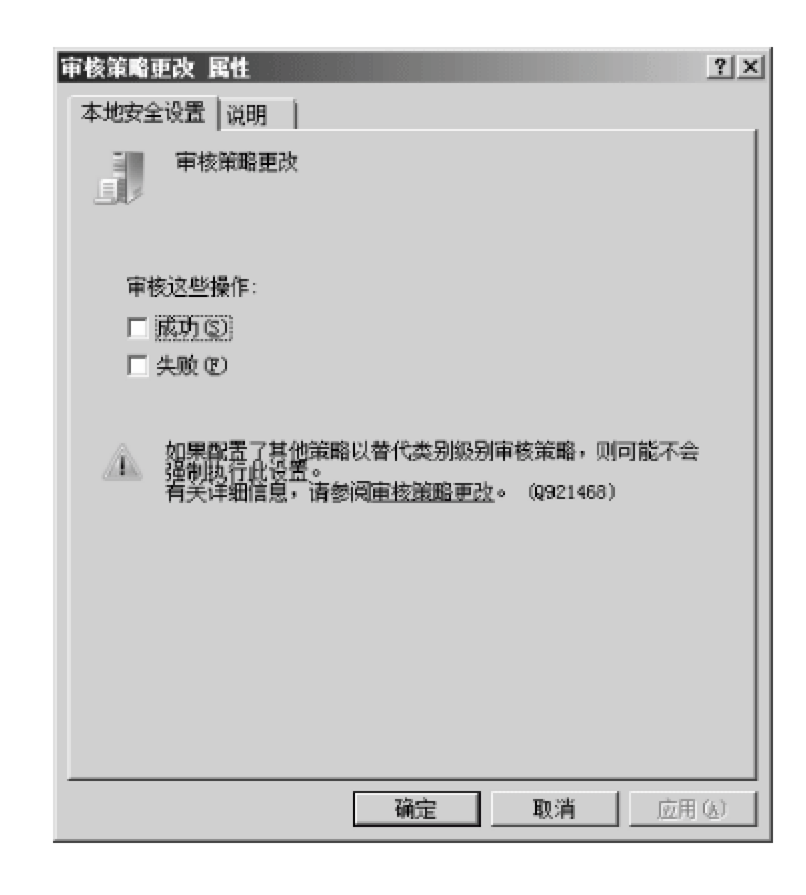


图 4-37 “审核策略更改 属性”对话框

(3) 设置完成后，单击“确定”按钮，保存设置。

注意：策略设置完成后，并不会立即生效，需要在系统更新组策略后才能生效，或运行 gpupdate /force 命令，手动刷新组策略。

5. 审核登录事件

设置审核登录事件，当在域控制器上对域用户账户进行身份验证时，将产生账户登录事件，该事件记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件，该事件记录在本地安全日志中，不产生账户注销事件。具体策略的设置方法同审核策略更改方法相同。

6. 审核文件的访问行为

审核文件的访问行为，可以审核某个或某些用户是否访问了某个文件或文件夹。只有当用户通过审核时，才可以访问该文件或文件夹，否则将不能访问该文件或文件夹。通过设置该审核策略，可以保证某些文件不被某些用户访问。具体策略的设置方法同审核策略更改方法相同，这里设置审核值为“成功”。

策略设置完成后，需要测试该策略是否能够起到审核作用，这里以设置文件夹的审核为例进行介绍，具体操作步骤如下。

(1) 打开 Windows 资源管理器，右击想要审核的文件或文件夹，在快捷菜单中选择“属性”命令，显示图 4-38 所示的对话框，并选择“安全”选项卡。

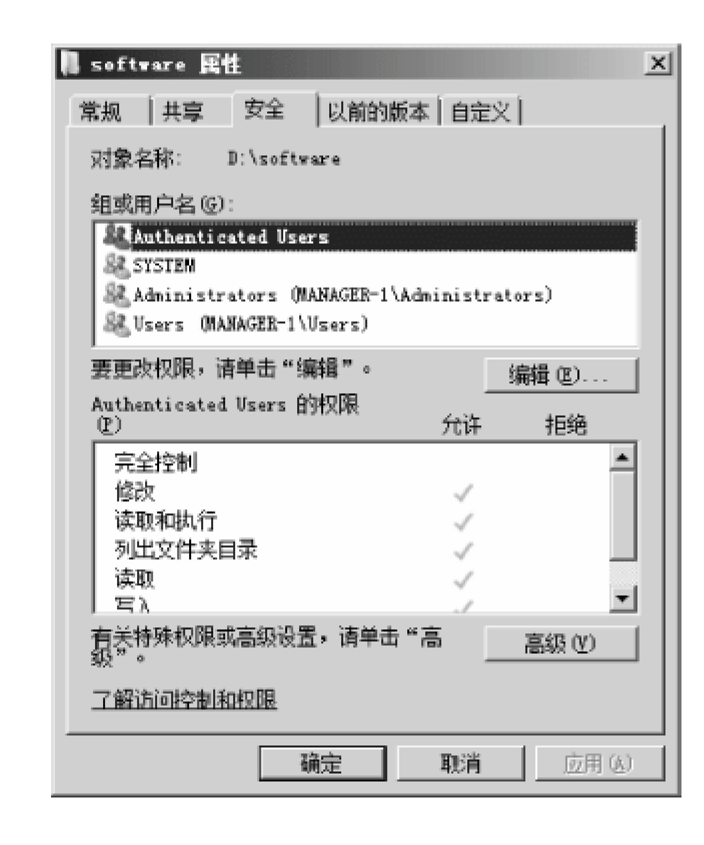


图 4-38 文件夹属性对话框

（2）单击“高级”按钮，显示图 4-39 所示的“software 的高级安全设置”对话框，选择“审核”选项卡，默认没有任何审核项目。单击“编辑”按钮，编辑审核项目。



图 4-39 “software 的高级安全设置”对话框

（3）单击“添加”按钮，打开“选择用户或组”对话框。单击“高级”按钮，显示图 4-40 所示的对话框，单击“立即查找”按钮即可开始查找用户，在“搜索结果”列表中，选择用户 czc。

小知识：如果用户知道想要审核的用户名详细名称，在“输入要选择的对象名称”文本框中直接输入该用户名称即可。

（4）单击“确定”按钮，显示图 4-41 所示的“software 的审核项目”对话框。在“访问”列表中，选择审核的操作，这里选中“创建文件夹/附加数据”和“删除”复选框。



图 4-40 “选择用户或组”对话框

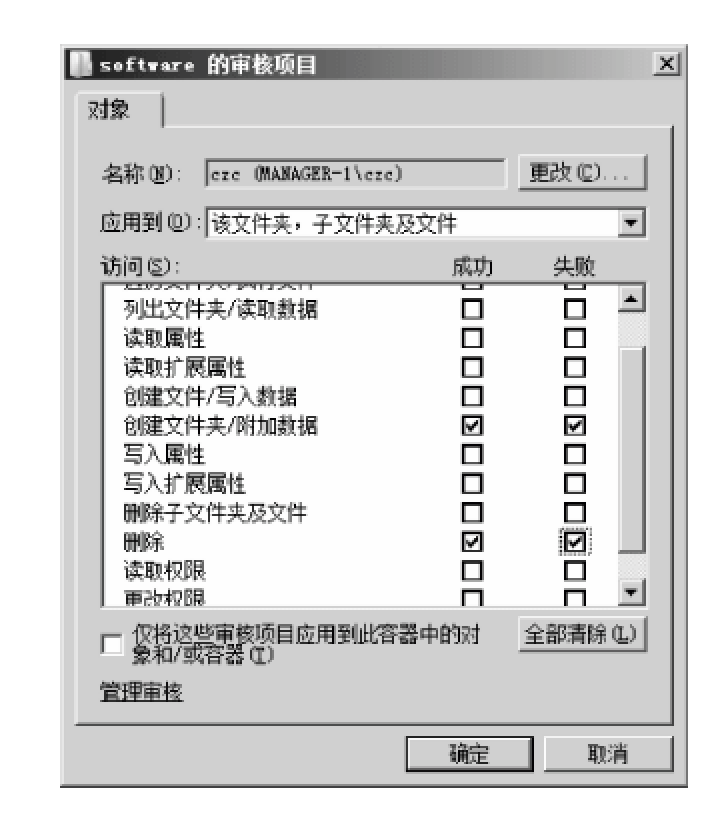


图 4-41 “software 的审核项目”对话框

（5）连续单击“确定”按钮，即可完成设置。

（6）注销当前登录的管理员账户，并以 czc 用户登录系统。在审核文件夹内创建名为 book 的文件夹，如图 4-42 所示。

(7) 注销 czc 用户,重新以管理员账户登录系统,以便查看审核日志。在“事件查看器”窗口中,选择“安全”日志事件,如图 4-43 所示。

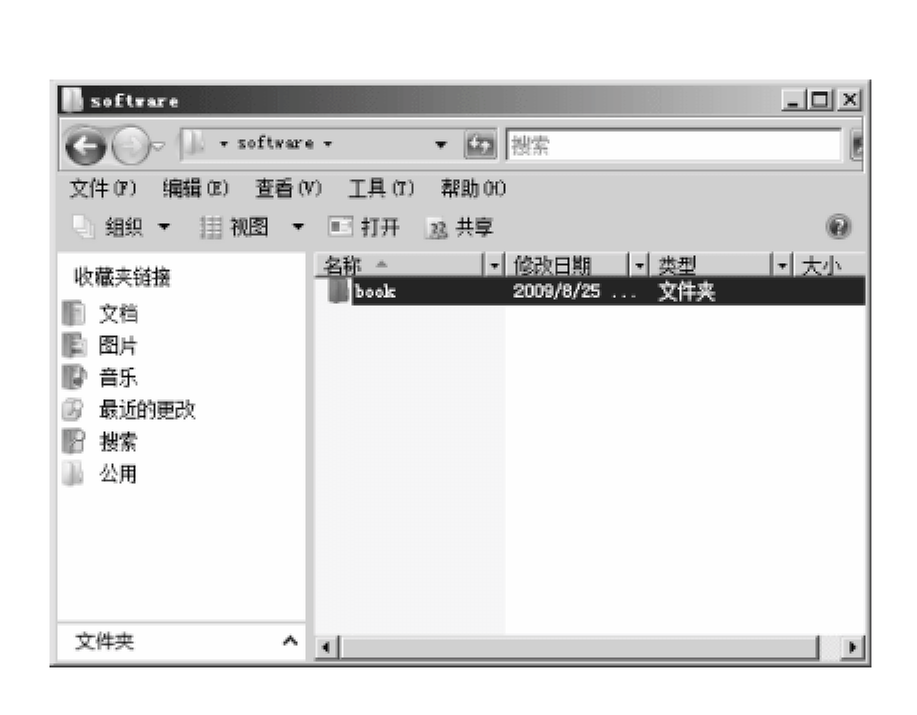






图 4-42　新建文件夹　　　　图 4-43　事件查看器

(8) 在右侧窗口中,双击所审核的事件日志,显示图 4-44 所示的“事件属性”对话框。从事件属性中可以看到,czc 用户创建文件夹的操作已经被记录下来。

7. 审核打印机的访问行为

审核打印机的访问行为,可以审核用户是否访问了某台打印机,例如该用户是否使用了该打印机打印文档等。审核打印机的访问行为,同样可以使用“事件查看器”的安全日志文件来查看这些事件日志。

启用“审核对象访问”策略,其操作步骤与“审核文件的访问行为”相同,这里就不再赘述。在“访问”列表中,根据需要选择审核内容,这里选中“打印”复选框。需要注意的是,在选中“打印”复选框的同时,系统会自动选中“读取权限”复选框,如图 4-45 所示。

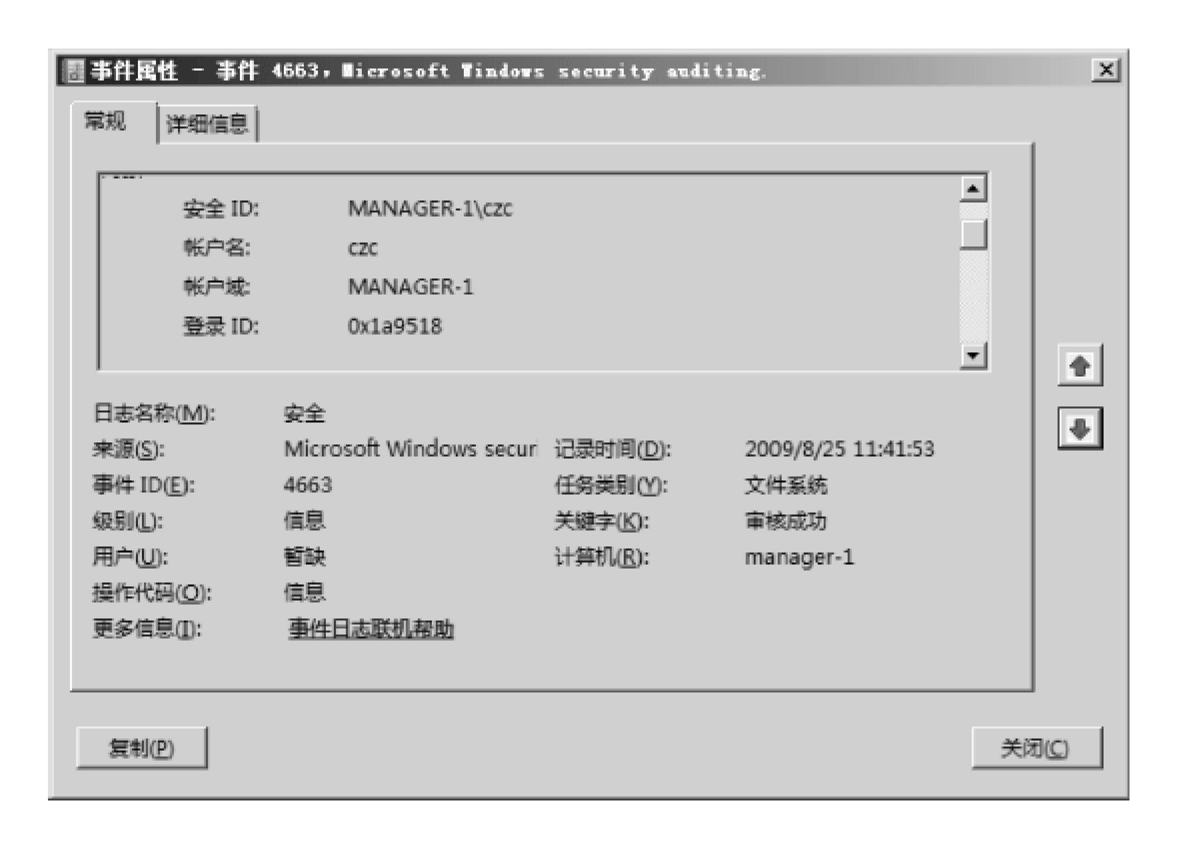




图 4-44　“事件属性”对话框　　　　图 4-45　审核打印机的访问行为

8. 用户权限分配

在大中型网络中,如果所有网络管理工具都由一名管理员来完成,其难度是非常大的。因此,通常情况下,在网络管理中会拥有一名权限最高的管理员,然后将部分安全功能设置权限分配给特定的用户账户,这样既可以减少系统或网络管理员的工作负担,又可以做到重

要权限的分散，避免了个别用户权限过高而给系统或网络带来的威胁。

在“本地组策略编辑器”窗口中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”目录，即可查看 Windows Server 2008 系统中的用户权限分配策略，如图 4-46 所示。

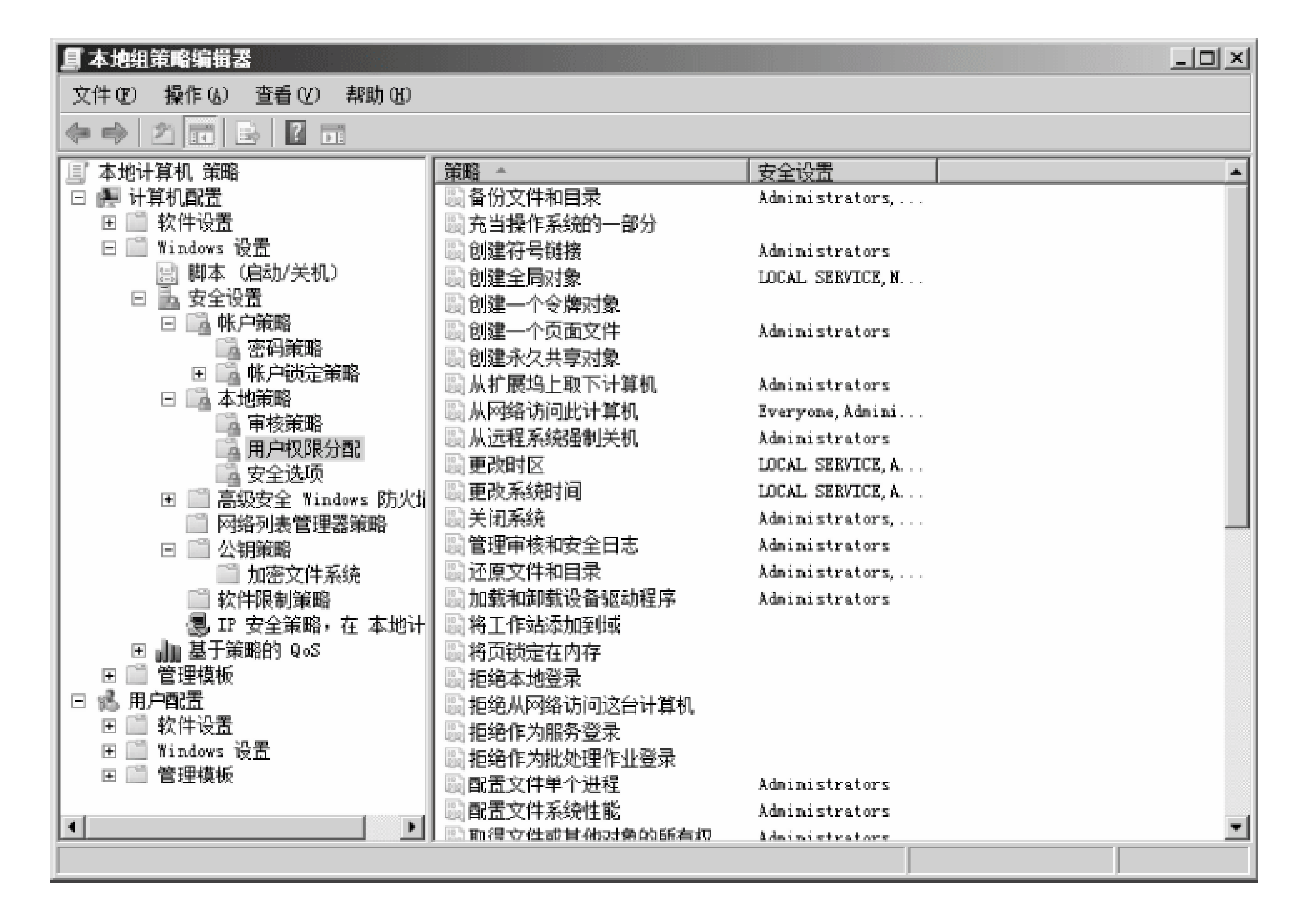


图 4-46 用户权限分配策略

在 Windows Server 2008 系统中，管理员可以为用户账户指派更为详细的安全管理权限，可分配权限及功能描述如表 4-1 所示。

表 4-1 用户权限分配策略及功能

策 略	功 能 说 明	默认用户账户和组
备份文件和目录	确定哪些用户可以绕过文件和目录、注册表和其他永久对象权限进行系统备份	Administrators、Backup Operators
充当操作系统的一部分	此用户权限允许某个进程模拟任意用户而无须进行身份验证。因此该进程可以与该用户一样获得对本地资源的访问权限	
创建符号链接	此权限决定用户是否可以从登录的计算机创建符号链接	Administrators
创建全局对象	此用户权限对于在终端服务会话过程中创建全局对象的用户账户是必需的。未分配此用户权限的用户仍可以创建特定于会话的对象	LOCAL SERVICE、NETWORK SERVICE、Administrators、SERVICE
创建一个令牌对象	此安全设置确定进程可以使用哪些账户创建令牌，该令牌接着可以在进程使用内部应用程序编程接口(API,Application Programming Interface)创建访问令牌时用于获取任何本地资源的访问权限。此用户权限供操作系统内部使用。除非必要，建议不要将此用户权限分配给本地系统之外的用户、组或进程	没有任何用户账户
创建一个页面文件	此用户权限确定哪些用户和组可以调用内部应用程序编程接口(API)创建页面文件。此用户权限供操作系统内部使用，且通常不需要分配给任何用户	Administrators

续表

策 略	功 能 说 明	默认用户账户和组
创建永久共享对象	此用户权限确定进程可以使用哪些账户，利用对象管理器创建目录对象。此用户权限供操作系统内部使用，且对于扩展对象命名空间的内核模式组件非常有用	没有任何用户账户
从扩展坞上取下计算机	此安全设置确定用户是否可以无须登录而从其扩展坞上移除便携式计算机	Administrators
从网络访问此计算机	此用户权限确定允许哪些用户和组通过网络连接到计算机。此用户权限不影响终端服务	Everyone、Administrators、Users、Backup Operators
从远程系统强制关机	此安全设置确定允许哪些用户从网络上的远程位置关闭计算机。误用此用户权限会导致拒绝服务。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Administrators
更改时区	此用户权限确定哪些用户和组可以更改计算机默认时区。这是 Windows Server 2008 的新增用户权限分配策略之一	LOCAL SERVICE、Administrators
更改系统时间	此用户权限确定哪些用户和组可以更改计算机内部时钟上的日期和时间。分配了此用户权限的用户可以影响事件日志的外观。如果已更改了系统时间，则记录的事件将反映此新时间，而不是事件发生的实际时间	LOCAL SERVICE、Administrators
关闭系统	此安全设置确定哪些在本地登录到计算机的用户可以使用关机命令关闭操作系统。误用此用户权限会导致拒绝服务	Administrators、Backup Operators
管理审核和安全日志	此安全设置确定哪些用户可以为单独的资源(如文件、Active Directory 对象和注册表项)指定对象访问审核选项	Administrators
还原文件和目录	此安全设置确定在还原备份的文件和目录时哪些用户可以绕过文件、目录、注册表和其他永久对象权限，以及确定哪些用户可以将任何有效的安全主体设置为对象的所有者	Administrators、Backup Operators
加载和卸载设备驱动程序	此用户权限确定哪些用户可以将设备驱动程序或其他代码动态加载和卸载到内核模式中。此用户权限不适用于即插即用设备驱动程序。建议不要将此权限分配给其他用户	Administrators
将工作站添加到域	此安全设置确定哪些组或用户可以将工作站添加到域。此安全设置仅对域控制器有效。默认情况下，任何已经过身份验证的用户都具有此权限并可以在该域中最多创建 10 个计算机账户	没有任何用户账户
将页锁定在内存	此安全设置确定哪些账户可以使用进程将数据保持在物理内存中，这样可防止系统将数据分页到磁盘上的虚拟内存中。使用此权限会因降低可用随机存取内存(RAM)的数量，而显著影响系统性能	没有任何用户账户
拒绝本地登录	此安全设置确定要防止哪些用户在该计算机上登录。如果账户受制于此策略设置和“允许本地登录”策略设置，则前者会取代后者	没有任何用户账户
拒绝从网络访问这台计算机	此安全设置确定要防止哪些用户通过网络访问计算机。如果用户账户受限于此策略设置和“从网络访问此计算机”策略设置，则前者会取代后者	没有任何用户账户

续表

策　略	功能说明	默认用户账户和组
拒绝作为服务登录	此安全设置确定要防止哪些服务账户将进程注册为服务。如果账户受制于此策略设置和“作为服务登录”策略设置，则前者会取代后者	没有任何用户账户
拒绝作为批处理作业登录	此安全设置确定要防止哪些账户作为批处理作业登录。如果用户账户受限于此策略设置和“作为批处理作业登录”策略设置，则前者会取代后者	没有任何用户账户
配置文件单个进程	此安全设置确定哪些用户可以使用性能监视工具来监视非系统进程的性能	Administrators
配置文件系统性能	此安全设置确定哪些用户可以使用性能监视工具来监视系统进程的性能	Administrators
取得文件或其他对象的所有权	此安全设置确定哪些用户可以取得系统中任何安全对象(包括 Active Directory 对象、文件和文件夹、打印机、注册表项、进程以及线程)的所有权	Administrators
绕过遍历检查	此用户权限确定哪些用户即使在不具有对已遍历目录的权限时，也可以遍历目录树。此权限不允许用户列出目录的内容，仅允许遍历目录。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Everyone、LOCAL SERVICE、NETWORK SERVICE、Administrators、Users、Backup Operators
身份验证后模拟客户端	将此权限分配给用户使代表该用户运行的程序能够模拟客户端。此种模拟要求此用户权限可防止未经授权的用户说服客户端连接(例如，通过远程过程调用(RPC)或命名管道)到他们已创建的服务，然后模拟该客户端，这样会将未经授权的用户的权限提升至管理级别或系统级别	LOCAL SERVICE、NETWORK SERVICE、Administrators、SERVICE
生成安全审核	此安全设置确定进程可以使用哪些账户将项目添加到安全日志中。安全日志用于跟踪未授权的系统访问。如果启用了“审核：如果无法记录安全审核，则立即关闭系统”安全策略设置，则误用此用户权限会导致生成许多审核事件，可能隐藏攻击证据或导致拒绝服务	LOCAL SERVICE、NETWORK SERVICE
提高计划优先级	此安全设置确定哪些账户可以使用对另一个进程具有 Write Property 访问权限的进程来提高分配给其他进程的执行优先级。具有此权限的用户可以通过任务管理器用户界面更改进程的计划优先级	Administrators
替换一个进程级令牌	此安全设置确定哪些用户账户可以调用应用程序编程接口，从而使一个服务能够启动另一个服务。任务计划程序是使用此用户权限的进程的一个示例	LOCAL SERVICE、NETWORK SERVICE
调试程序	此用户权限确定哪些用户可以将调试程序连接到任何进程或连接到内核。不需要将此用户权限分配给正在调试自己的应用程序的开发人员。调试新系统组件的开发人员将需要此用户权限来执行相应操作。此用户权限提供对敏感和关键系统组件的完全访问权限	Administrators
通过终端服务拒绝登录	此安全设置确定禁止哪些用户和组作为终端服务客户端登录	没有任何用户账户
通过终端服务允许登录	此安全设置确定哪些用户或组具有作为终端服务客户端登录的权限	Administrators、Remote Desktop Users
同步目录服务数据	此安全设置确定哪些用户和组有权同步所有目录服务数据，也称为 Active Directory 同步	没有任何用户账户

续表

策　略	功 能 说 明	默认用户账户和组
为进程调整内存配额	此权限确定哪些用户可以更改进程可消耗的最大内存。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	LOCAL SERVICE、NETWORK SERVICE、Administrators
信任计算机和用户账户可以执行委派	此安全设置确定哪些用户可以在用户或计算机对象上，设置“已为委派信任”设置	没有任何用户账户
修改固件环境值	此安全设置确定哪些用户可以修改固件环境值。固件环境变量是在非基于 x86 的计算机的稳定 RAM 中存储的设置。该设置的效果依赖于处理器	Administrators
修改一个对象标签	此权限决定哪些用户账户可以修改对象(例如文件、注册表项或其他用户所拥有的进程)的完整性标签。在用户账户下运行的进程可以将该用户所拥有的对象标签修改为没有此权限的更低级别	没有任何用户账户
允许在本地登录	此登录权限确定哪些用户能以交互方式登录到此计算机。通过在连接的键盘上按 Ctrl+Alt+Delete 键启动的登录要求用户具有此登录权限。此外，可以登录用户的某些服务或管理应用程序可能要求此登录权限。如果为某个用户或组定义此策略，则还必须向 Administrators 组授予此权限	Administrators、Users、Backup Operators
增加进程工作集	此安全设置确定允许那些用户增加运行进程时所需访问的页面数量	Users
执行卷维护任务	此安全设置确定哪些用户和组可以在卷上运行维护任务，如远程碎片整理。需要注意的是，具有此用户权限的账户可以浏览磁盘及将文件扩展到包含其他数据的内存中。当打开扩展的文件时，用户可能能够读取和修改获得的数据	Administrators
作为服务登录	此安全设置确定哪些服务账户可以将进程注册为服务	没有任何用户账户
作为批处理作业登录	此安全设置使用户能够通过批处理队列实用程序登录，并仅提供用于与旧版本的 Windows 的兼容性	Administrators、Backup Operators、Performance Log Users
作为受信任的呼叫方访问凭据管理器	此安全设置用于确定哪些远程访问账户可以访问本地服务器或网络上的凭据管理器，存在很大的风险，建议不要轻易使用	没有任何用户账户

这里以“备份文件和目录”为例，介绍如何配置用户权限分配策略。主要操作步骤如下。

(1) 双击“备份文件和目录”策略，打开“备份文件和目录 属性”对话框，列表中显示的是策略默认的用户账户和组。

(2) 单击“添加用户或组”按钮，显示图 4-47 所示的“选择用户或组”对话框。在“输入对象名称来选择”文本框中输入想要添加的用户账户或组。

(3) 单击“确定”按钮，即可将其添加至策略允许的对象列表中，如图 4-48 所示。

(4) 单击“确定”按钮，保存设置即可。使用相同的方法即可定义其他用户权限分配策略，此处不再赘述。



图 4-47 “选择用户或组”对话框



图 4-48 成功为权限添加用户账户

4.3 系统日志

Windows 日志类别包括以下在早期版本的 Windows 中可用的日志：应用程序、安全和系统日志，还包括两个新的日志：安装程序日志和 ForwardedEvents 日志。Windows 日志用于存储来自旧版应用程序的事件以及适用于整个系统的事件。

4.3.1 事件查看器

事件查看器也是系统日志的一种形式。虽然“事件查看器”主要是一个管理员用来管理事件日志的工具，但用户也可以查看自己计算机上的应用程序和系统日志。

1. 查看事件的详细信息

选中“事件查看器”左边的树型结构图中的日志类型(应用程序、安全或系统)，在右侧的详细资料窗格中将会显示出系统中该类的全部日志，双击其中一个日志，便可查看其详细信息。在日志属性窗口中可以看到事件发生的日期、事件的发生源、种类和 ID，以及事件的详细描述。这对寻找解决错误是最重要的。

(1) 查看事件信息

① 依次选择“开始”→“管理工具”→“事件查看器”命令，打开“事件查看器”窗口，并展开左侧栏“Windows 日志”目录，即可详细查看系统日志，如图 4-49 所示。

② 在左侧“事件查看器”目录中，单击想要查看的事件类型，在右侧主窗口中显示该类型的所有事件日志及其日期。根据事件日志的发生日期和具体时间，选择并双击想要查看的日志记录，即可显示图 4-50 所示的“事件属性”对话框。

③ 选择“详细信息”选项卡，如图 4-51 所示，系统默认是以“友好视图”方式显示的。

④ 选中“XML 视图”单选按钮，即可以“XML 视图”方式显示事件详细信息，如图 4-52 所示。

⑤ 单击“关闭”按钮，关闭“事件属性”对话框即可。



图 4-49　事件查看器



图 4-50　“事件属性”对话框

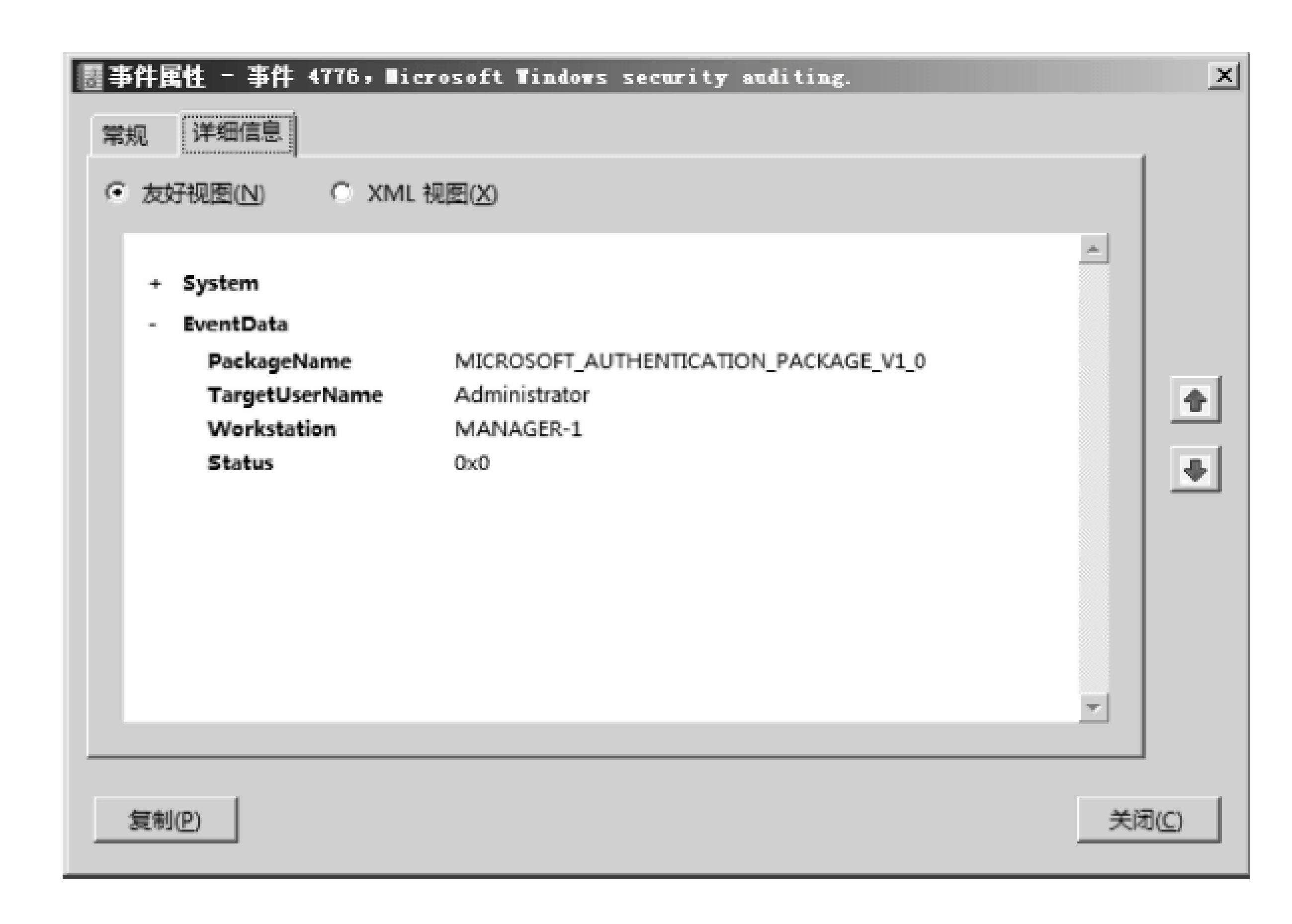


图 4-51　“友好视图”方式显示

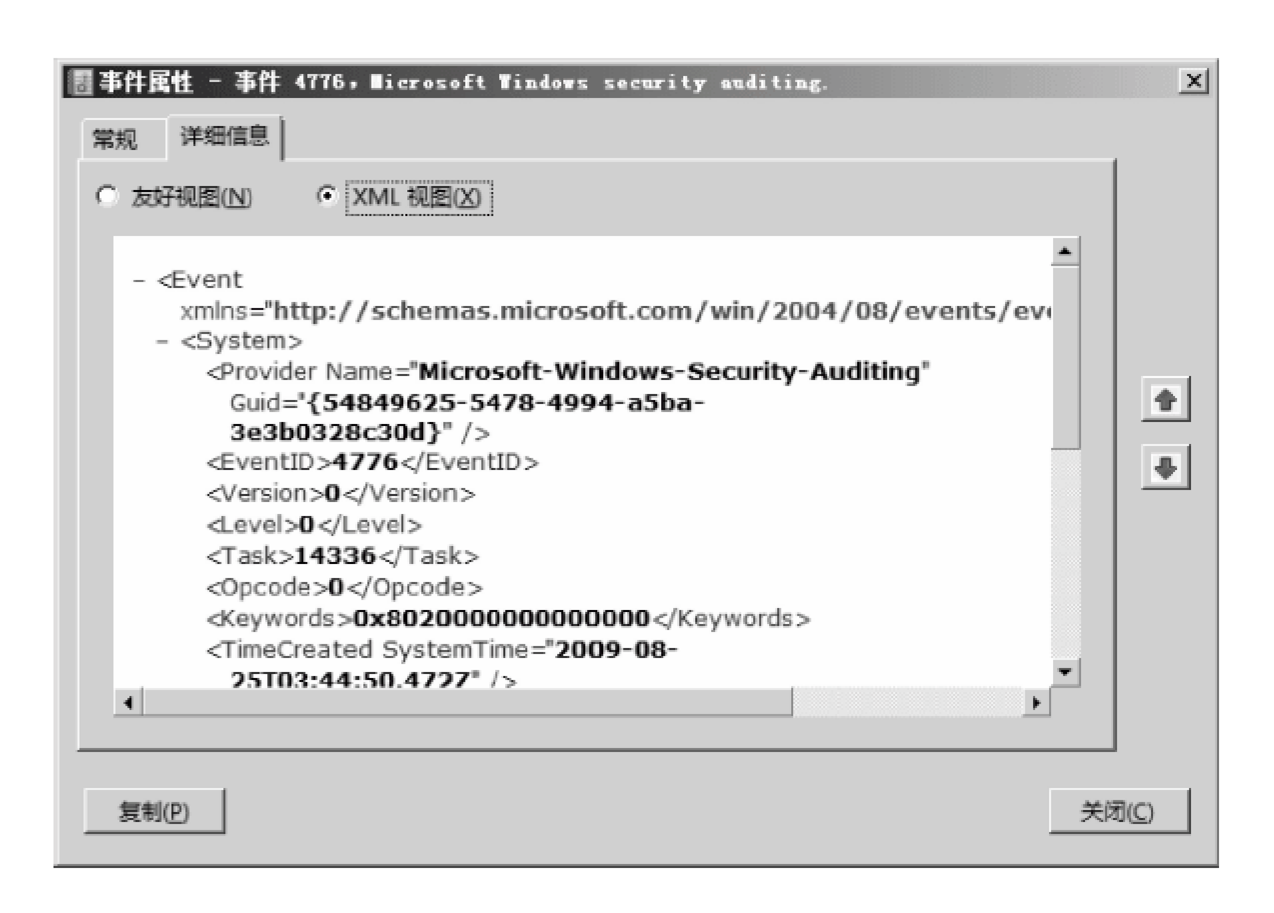


图 4-52 “XML 视图”方式显示

(2) 查看远程计算机事件日志

默认状态下，在“事件查看器”控制台窗口中显示的都是本地计算机系统的事件日志，根据需要还可以查看其他计算机的事件日志。

在“事件查看器”控制台中，右击“事件查看器(本地)”并选择快捷菜单中的“连接到另一台计算机”命令，显示图 4-53 所示的“选择计算机”对话框，选中“另一台计算机”单选按钮，并在其文本框中输入目标计算机的主机名或 IP 地址。

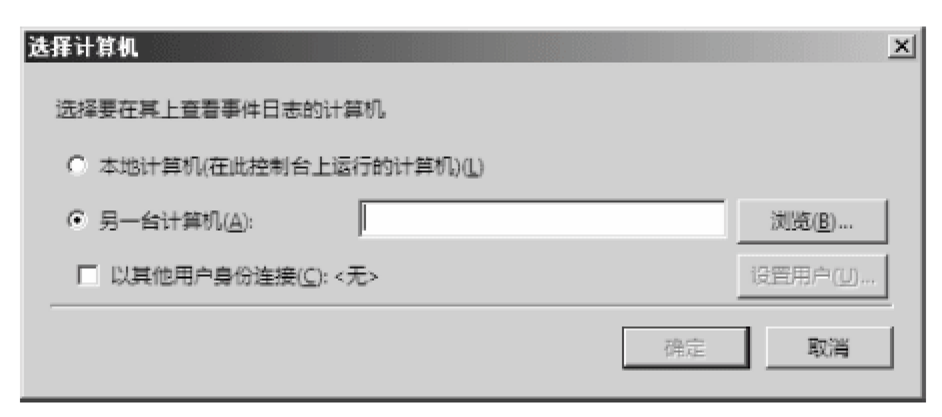


图 4-53 “选择计算机”对话框

单击“确定”按钮，如果网络连接正常，即可在控制台窗口中显示远程计算机的“事件查看器”内容。查看远程主机事件详细信息的方法，与查看本地计算机事件完全相同。需要注意的是，如果要想查看远程主机的“安全”事件信息，必须以管理员或 Administrators 组成员的身份登录。

提示：若不清楚目标主机的计算机名和 IP 地址，还可以单击“浏览”按钮进行搜索。另外，该功能仅能在域环境中使用。

2. 管理事件日志

事件日志的产生是自动的，但是日积月累占用系统空间也会越来越多，这会严重影响服务器的运行速度，甚至会丢失早期重要的事件日志。管理事件日志主要就是清除陈旧无用的信息，并导出重要信息妥善保管，以便日后查看。用户可以对本地计算机或远程计算机的事件日志进行管理。

(1) 删除时间日志

删除日志时，系统首先删除包含该日志内容的文件，然后访问注册表并将注册到此日志的所有事件源的注册都移除。因此即使重新创建已被删除日志，也不会以默认方式创建这些源。删除相关事件日志之前，必须保证当前操作用户账户拥有足够的操作权限。需要注意的是，重新创建事件日志是一个相当麻烦的过程，因此建议不要删除任何由系统创建的事件日志(如“系统”日志)。可以根据需要删除和重新创建自定义日志。

打开“事件查看器”窗口，在左侧目录中选择想要删除的事件日志的类型，然后单击“操作”按钮并选择“清除日志”命令，显示图 4-54 所示的对话框。提示在清除之前是否要保存这些事件日志，如果想要彻底删除这些事件日志，则可以直接单击“清除”按钮；如果在清除之前想要保存该日志，可以单击“保存并清除”按钮将其导出。



图 4-54　删除事件日志提示

提示：必须以管理员或 Administrators 组成员的身份登录才能清除事件日志。清除日志后，日志中将只显示新的事件。不能清除存档日志，而是删除存档的日志文件。

(2) 导出事件日志

如果 Windows 服务器的访问量非常大，则每天产生的日志文件大小也是非常惊人的，尽管安装 Windows 系统和网络服务时，已经选择了安全可靠的日志保存目录，但为了确保日志文件的完整、安全，应适时将其备份至安全性较高的存储介质，如光盘或其他文件服务器等，以免由于系统故障或日志文件自动覆盖，而丢失重要信息。另外，事件日志是管理员诊断和排除服务器故障的重要依据，因此对于一些重要的系统日志如果仍然采取统统删除的手段，显然是不可取的。为了释放系统和磁盘空间，可以将其暂时导出保存，需要的时候还可以导入查看。

在“事件查看器”窗口中，单击要导出保存的事件类型，如“系统”日志，然后选择“操作”菜单中的“将事件另存为”命令，打开图 4-55 所示的对话框，并在“文件名”文本框中输入合适的文件名。

如果以日志文件格式存档日志，则可以在“事件查看器”窗口中重新打开。另存为事件日志文件(*.evtx)的日志，将保留所记录的每个事件的二进制数据。把日志存档为文本表格的格式(分别为 *.txt 和 *.csv)，还可以在 Office Excel 或其他文字处理软件中重新打开日志。把日志保存为配置文件格式(*.xml)，可以在 IE 浏览器中浏览日志信息。

单击“保存”按钮，显示图 4-56 所示的“显示信息”对话框。如果想要在其他计算机上正确查看该日志信息，可以选中“显示这些语言的信息”单选按钮，并设置所显示的语言信息。

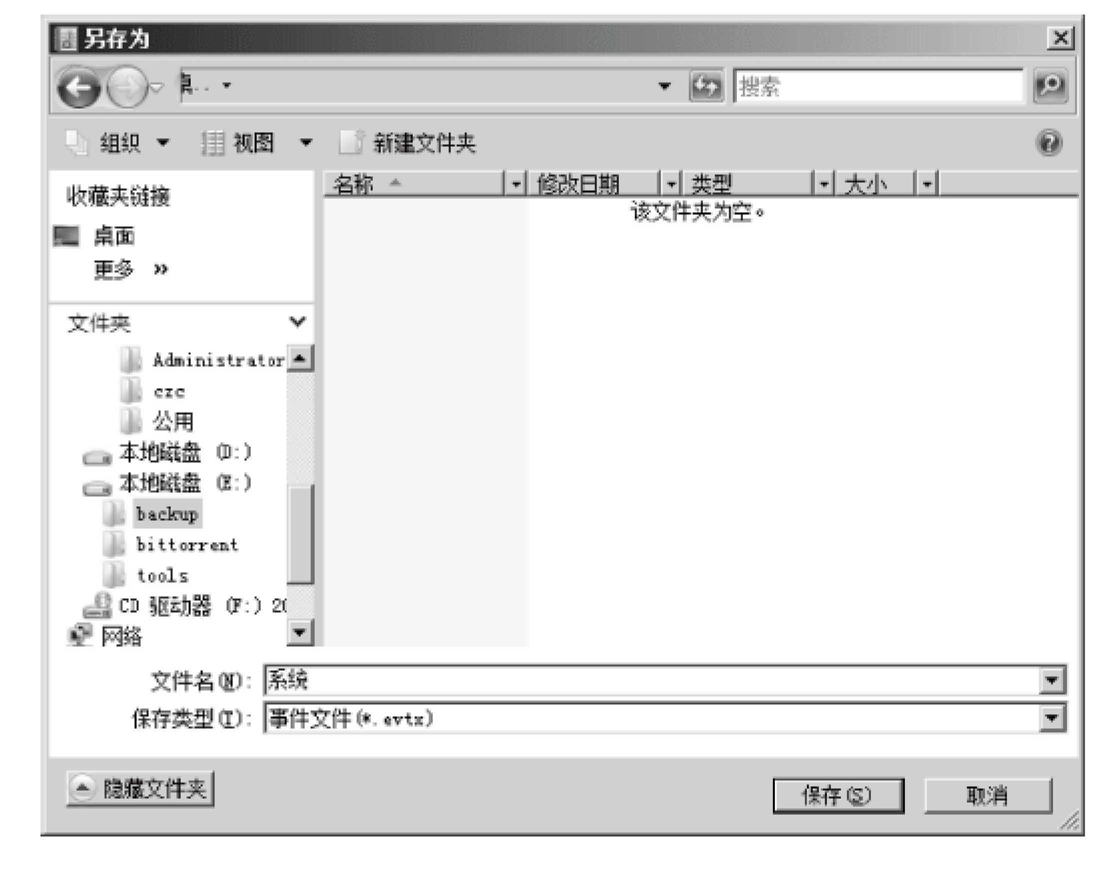


图 4-55　保存事件日志

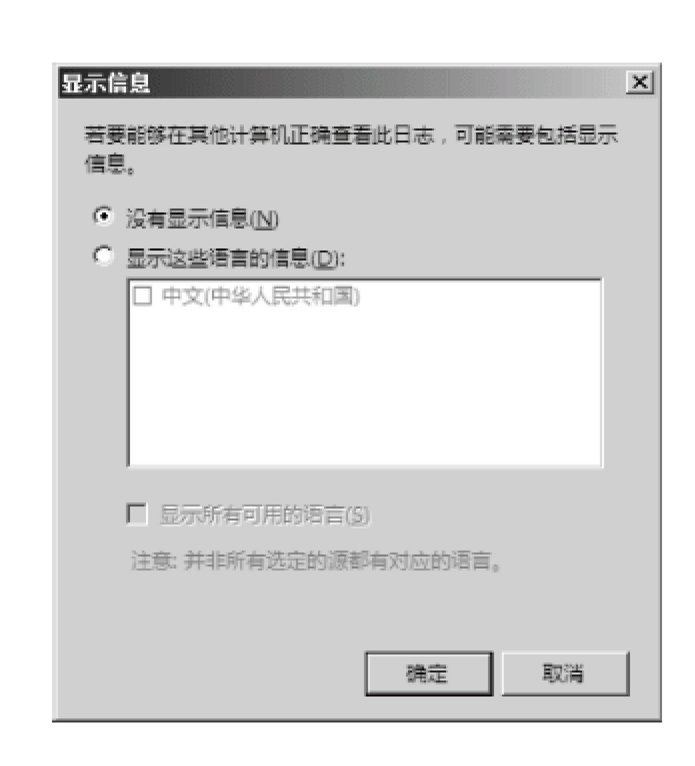


图 4-56　“显示信息”对话框

提示：将日志文件存档时，不管筛选选项如何设置，整个日志都被保存。保存日志时不保留排序顺序。存档对当前的活动日志内容无效。

(3) 查看存档事件日志

查看曾经保存过的事件日志，首先必须打开“事件查看器”控制台窗口，然后选择“操作”菜单中的“打开保存的日志”命令，显示图 4-57 所示的“打开保存的文件”对话框，需要注意的是，打开存档事件之前必须指定其日志类型，单击“文件名”右侧的下拉按钮选择对应类型即可。



图 4-57 “打开保存的文件”对话框

只有当日志是以日志文件格式(.evtx)保存时，才能在“事件查看器”中查看已存档的文件。打开保存的事件日志后是不可以进行刷新或删除的。

3. 将任务附加到事件

Windows Server 2008 系统的“事件查看器”新增了通知、提醒功能，通过将任务计划附加到指定类型的事件，系统即可自动以某种方式通知用户，如发送 E-mail 邮件、弹出提示信息、开启程序等。可以选择一类系统事件作为关联对象，也可以选择单个事件进行关联。将任务附加到一类事件的具体操作步骤如下。

(1) 在“事件查看器”窗口中，右击“安装程序”链接(此处以“安装程序”类别的 Windows 事件为例)，并在快捷菜单中选择“将任务附加到事件”命令，启动“创建基本任务向导”，显示图 4-58 所示的“创建基本任务向导”对话框。这里使用系统默认名称，并在“描述”文本框中输入对此基本任务的简单描述，以便区分。

(2) 单击“下一步”按钮，显示“登录特定事件时”对话框。当出现定义的事件时，将发生的动作。

(3) 单击“下一步”按钮，显示图 4-59 所示的“操作”对话框。定义当事件发生后，希望发生的操作，本例中选中“发送电子邮件”单选按钮。

(4) 单击“下一步”按钮，显示图 4-60 所示的“发送电子邮件”对话框。在“发件人”和“收件人”文本框中输入希望使用的 E-mail 邮箱地址。在“正文”文本框中可以输入简短的描述信息，告知用户发送此邮件的目的。

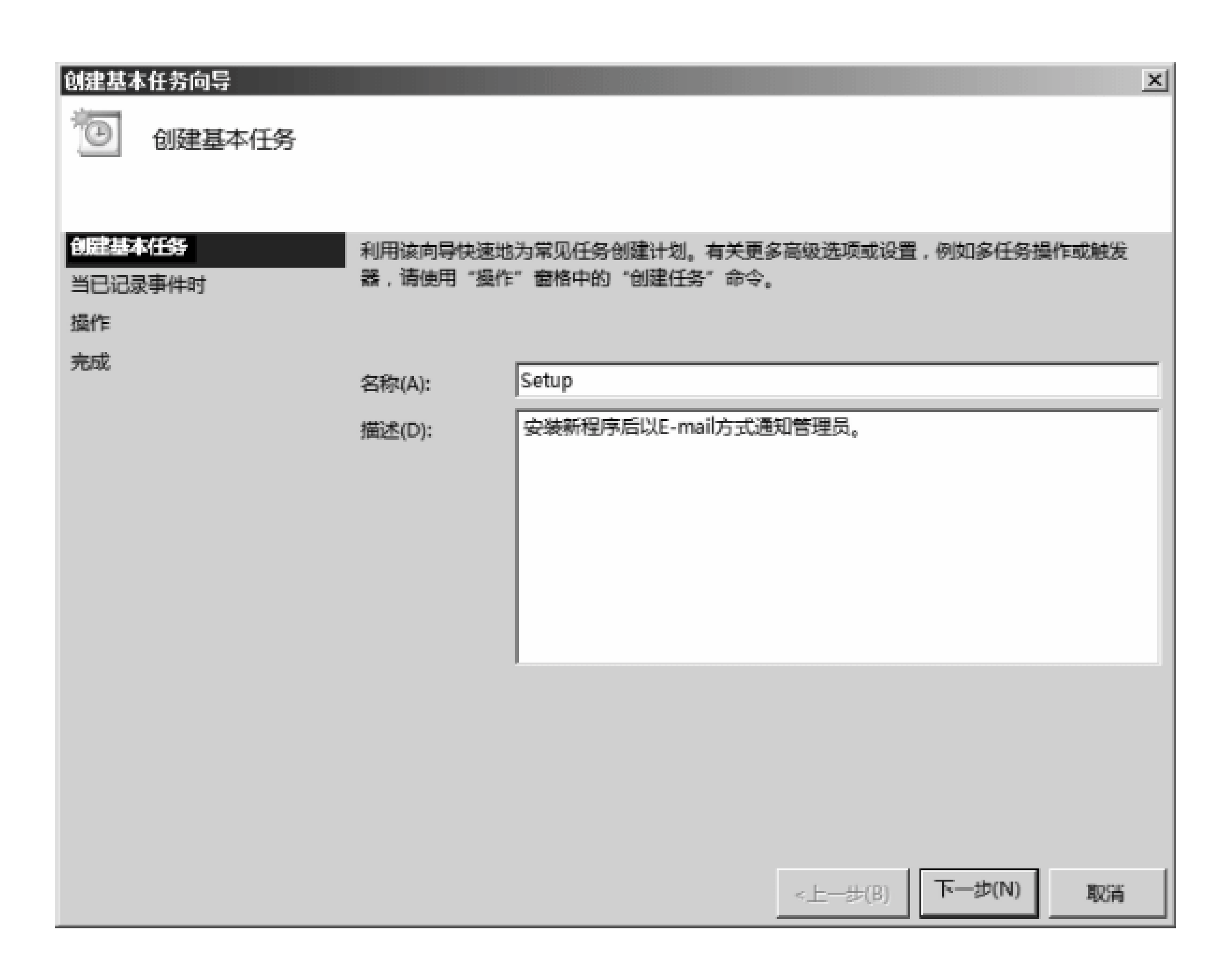


图 4-58 “创建基本任务向导”对话框



图 4-59 “操作”对话框

(5) 单击“下一步”按钮，显示图 4-61 所示的“摘要”对话框，提示当前已做的所有设置。如果选中“当单击‘完成’时，打开此任务属性的对话框”复选框，则关闭“创建基本任务向导”后，可以立即查看和编辑其属性设置。

(6) 单击“完成”按钮，打开图 4-62 所示的“事件查看器”提示对话框，提示计划任务已创建完成，可以在“任务计划程序”中查看和编辑计划的任务。

(7) 单击“确定”按钮，关闭对话框即可。



图 4-60 “发送电子邮件”对话框

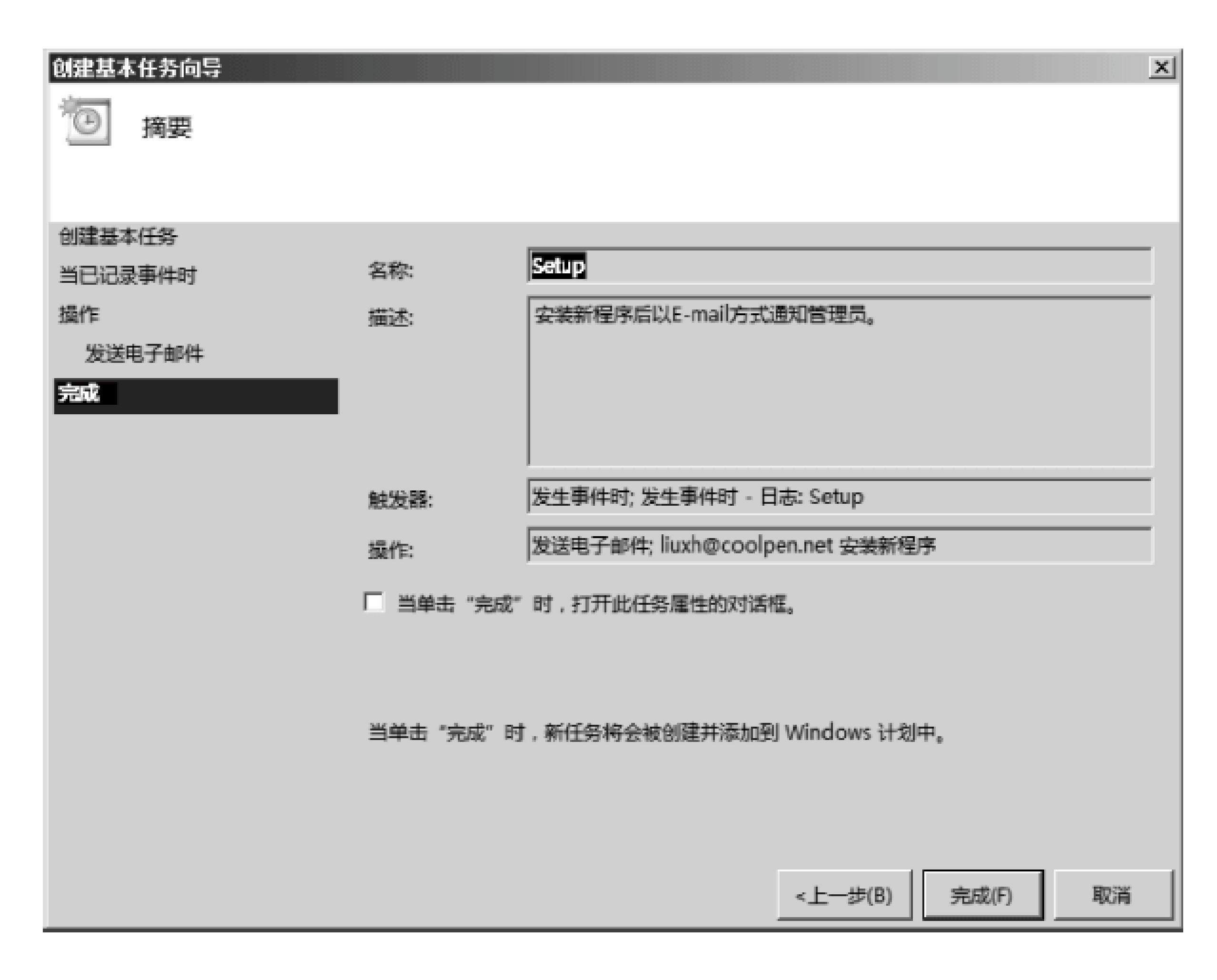


图 4-61 “摘要”对话框

提示：在 Windows Server 2008 系统中，可以通过依次选择“开始”→“管理工具”→“任务计划程序”命令，打开“任务计划程序”管理器，在这里管理员可以对系统中所有的计划任务进行配置和管理。在“事件查看器”中创建的任务关联也会显示在这里，如图 4-63 所示。

通过“创建基本任务向导”创建的任务关联计划，默认只能设置单一的“触发器(即执行任务的条件)”和“动作”。例如，在“任务计划程序”窗口中，双击已创建的关联任务计划(以 Setup 为例)，打开“Setup 属性”对话框，选择“操作”选项卡，单击“新建”按钮，打开“新建操作”对话框，在“操作”下拉列表框中，继续选择希望执行的操作类型即可，如图 4-64 所示。

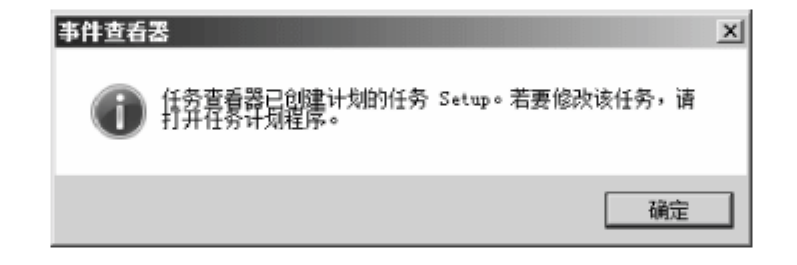


图 4-62 “事件查看器”提示对话框

4. 分析日志和调试日志

分析日志和调试日志主要面向 IT 专业用户提供，用于分析事件产生的原因、过程等因素，对普通用户的



图 4-63 “任务计划程序”窗口



图 4-64 “新建操作”对话框

正常应用没有太大影响。因此，默认情况下分析日志和调试日志为禁用和隐藏状态。用户可以打开“事件查看器”窗口，然后选择“查看”菜单中的“显示分析和调试日志”命令，即可在“应用程序和服务日志”目录中看到相关的事件日志，如图 4-65 所示。

4.3.2 系统日志设置

正因为系统日志有如此重要的作用，妥善保存这些日志记录成为管理员日常维护的一项重要工作。默认状态下，系统日志的存储空间、保存方法、保存日期都是有一定限制的，如果系统事件较多，时间长了很可能会造成存储溢出，即导致部分事件记录被自动清除。因



图 4-65　显示分析和调试日志

此，通常情况下需要对系统日志进行如下设置。

1. 设置系统日志选项

在“事件查看器”控制台中，右击需要配置选项的日志类型，如“应用程序”事件日志，在快捷菜单中选择“属性”命令，显示图 4-66 所示的“日志属性”对话框。



图 4-66　设置事件日志选项

(1) 日志路径：当前日志的保存路径。

(2) 日志最大大小(KB)：当前事件日志在计算机磁盘中被分配的磁盘空间，可以根据服务器类型判断日志文件的大小，从而设定合适的空间上限，建议设置较大的空间上限，以免由于磁盘空间不足而自动删除未经保存的陈旧事件日志。

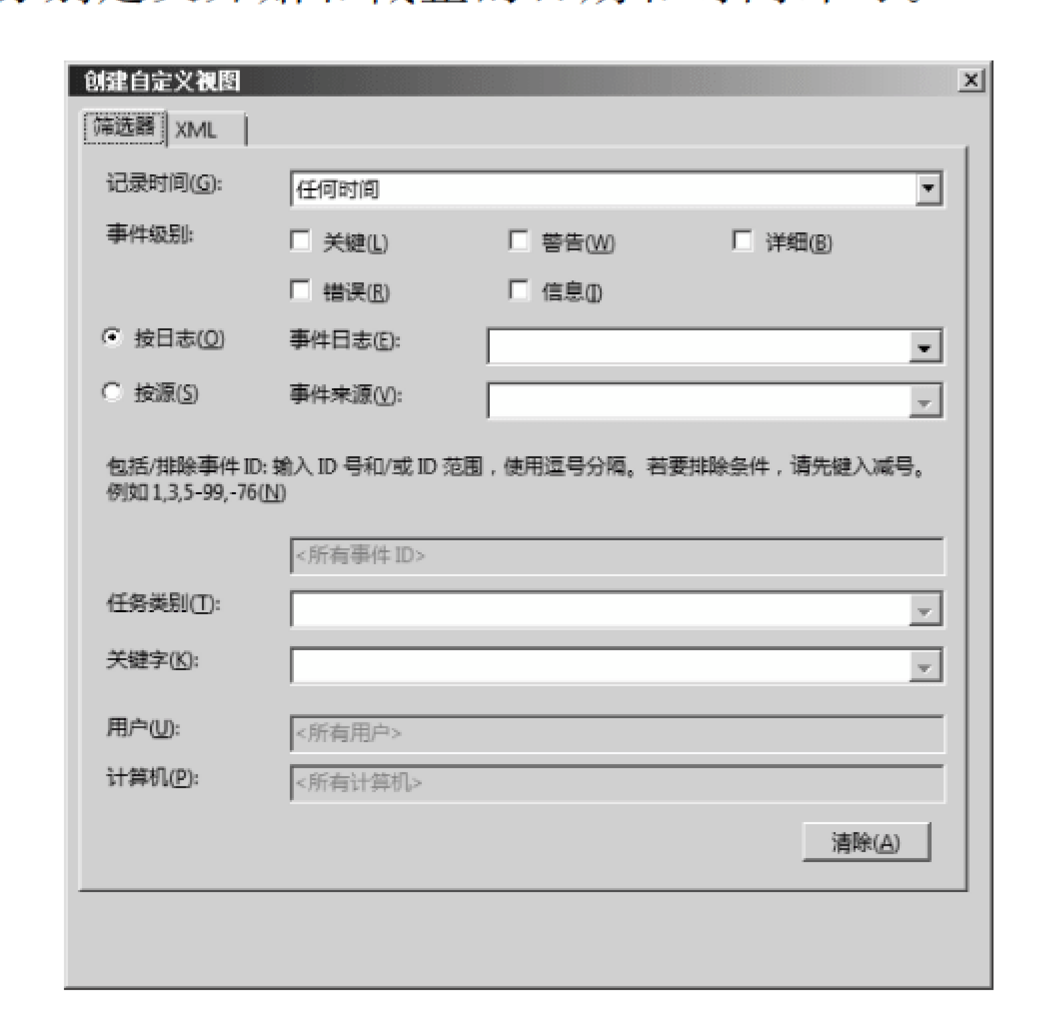
(3) 达到事件日志最大大小时：当达到日志大小上限时，系统将按照默认或预先设定的动作执行，系统默认的是“按需要覆盖事件”。

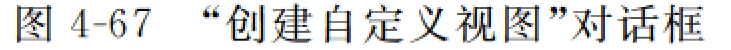
2. 创建自定义视图

通常情况下，服务器运行过程中会产生大量的事件日志，如果逐个查看这些事件则需要花费很长的时间，而其中大部分都是记录访问或操作成功的日志，对于管理员的安全管理工作意义不大。自定义视图的功能类似于"筛选"，通过创建自定义视图，可以指定自己希望查看的事件。例如只显示错误事件和警告事件，正常的事件将不需要显示。

(1) 以管理员账户登录服务器，打开"事件查看器"窗口，选择"自定义视图"类别，并在"操作"菜单中选择"创建自定义视图"命令，打开图 4-67 所示的"创建自定义视图"对话框。

(2) 在"记录时间"下拉列表框中选择日志产生的时间，系统默认为"任何时间"，用户还可以选择"前 1 个小时"、"过去的 24 小时"、"最后的 7 天"等时间，或者选择"自定义范围"选项，打开图 4-68 所示的"自定义范围"对话框，设置希望查看日志产生的时间范围。例如，按照事件产生的时间设置，首先，分别在"从"和"到"下拉列表框中选择"事件时间"选项，然后再分别定义开始和截止的日期和时间即可。




图 4-67 "创建自定义视图"对话框

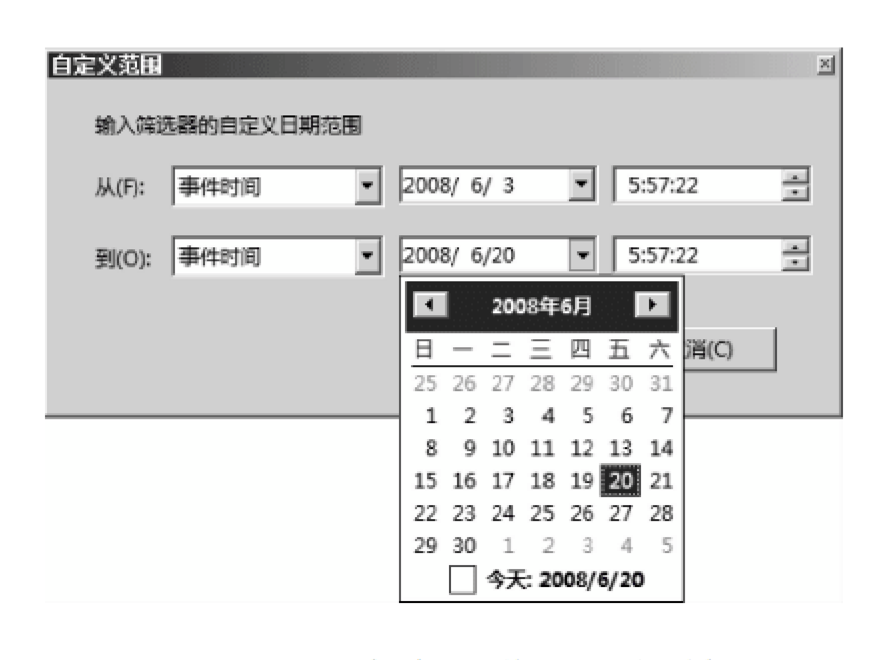


图 4-68 "自定义范围"对话框

(3) 单击"确定"按钮返回"创建自定义视图"对话框，在"事件级别"选项区域选择事件的级别，例如"警告"和"错误"。

(4) 选中"按日志"单选按钮，并在"事件日志"下拉列表框中依次选中"Windows 日志"→"安全"复选框，如图 4-69 所示。

(5) 单击"确定"按钮，显示图 4-70 所示的"将筛选器保存到自定义视图"对话框，输入自定义视图的名称，以及自定义视图在事件查看器中的位置。

(6) 单击"确定"按钮，完成自定义视图的创建，如图 4-71 所示。在事件列表中，显示的所有事件级别全部是"错误"。

4.3.3 知识链接：Windows 的日志类别

Windows 日志的类别如下。



图 4-69 选择事件来源

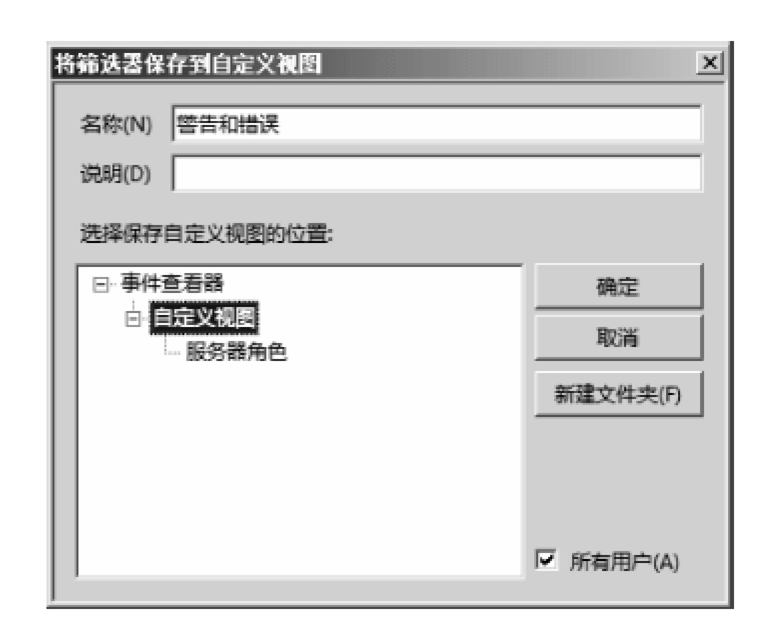


图 4-70 “将筛选器保存到自定义视图”对话框



图 4-71 “服务器管理器”窗口

1. 应用程序日志

应用程序日志包含由应用程序或程序记录的事件，例如，数据库程序可在应用程序日志中记录文件错误。程序开发人员决定记录哪些事件。

2. 安全日志

安全日志包含诸如有效和无效的登录尝试等事件，以及与资源使用相关的事件，如创建、打开或删除文件或其他对象。管理员可以指定在安全日志中记录什么事件，例如，如果已启用登录审核，则对系统的登录尝试将记录在安全日志中。

3. 安装程序日志

安装程序日志包含与应用程序安装有关的事件。

4. 系统日志

系统日志包含 Windows 系统组件记录的事件,例如,在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。系统组件所记录的事件类型由 Windows 预先确定。

5. ForwardedEvents 日志

ForwardedEvents 日志用于存储从远程计算机收集的事件。若要从远程计算机收集事件,必须创建事件订阅。

习题

1. 本地安全策略包括哪些内容?
2. Windows 日志包括哪几类日志?

实验:熟练安全配置向导的使用

实验目的:

掌握使用安全配置向导配置系统安全策略。

实验内容:

配置服务器的网络安全策略及注册表安全策略,保存并应用安全策略。

实验步骤:

(1) 启动安全配置向导,确认创建新策略。

(2) 选择所要配置的服务器。

(3) 选择服务器角色。

(4) 选择客户端功能。

(5) 选择管理和其他选项。

(6) 选择其他服务。

(7) 配置网络安全策略。

(8) 设置注册表。

(9) 设置审核策略。

(10) 保存安全策略。

(11) 应用安全策略。

第 5 章 chapter 5

Windows网络服务管理

Windows Server 2008 作为服务器操作系统，其主要任务就是为网络提供各种服务，如IIS 服务、DHCP 服务、DNS 服务等。为了最大限度地使用系统资源，需要控制系统服务的运行状态，这不仅事关服务器的系统性能，而且事关服务器的系统安全，也是系统管理员系统维护工作的重要组成部分。

5.1 Windows 网络服务规划

网络的主要特点是网络共享，这也是网络的主要功能，要实现该功能，必须在网络中拥有提供服务的服务器。针对于不同的网络需求，在网络中需要安装的网络服务也就不同，例如，为了共享文件，可在网络中安装文件服务器。

5.1.1 项目背景

在当前网络中，几乎所有的网络服务均安装在 Windows Server 2008 操作系统中，即几乎所有的服务平台均采用 Windows Server 2008 操作系统。而对于服务器状态的监控，则选择使用第三方的软件，将其安装在 Windows Server 2003 操作系统中。

5.1.2 项目需求

默认情况下，服务器操作系统安装完成后，不会安装任何服务组件，这些组件需要管理员根据需要进行选择性的安装。并且在安装多数服务时，如果使用默认的安装组件是不能满足网络要求的，还需根据需要安装所需的角色服务。另外，在网络中还存在一些对网络的稳定性和服务的稳定性要求比较高的网络服务，对于这些服务则必须使用相应的技术来实现。

5.1.3 解决方案

对于当前网络中网络服务的管理需求，可使用如下方案解决。

(1) 服务器角色和角色服务的安装，以及删除服务器角色均采用 Windows Server 2008 操作系统提供的“服务器管理器”来完成。

(2) 网络服务的管理可通过 MMC 控制台和相应服务所提供的独立管理窗口进行管理。

(3) 网络服务状态监控可通过使用第三软件 Servers Alive 和 OpManager 实现。

(4) 对于网络中安装比较重要的服务的服务器,可采用服务器群集技术实现故障转移,从而保证网络服务的稳定运行。

(5) 对于网络访问量比较大的服务器,则可采用网络负载平衡技术,合理地将访问量进行冗余。

5.2　网络服务的添加与删除

Windows Server 2008 的一个亮点就是组件化,所以微软使用"服务器管理器"替代了"管理您的服务器"。而 Windows Server 2003 中需要在"添加/删除 Windows 组件"和"配置您的服务器向导"中完成的操作,都可以在"服务器管理器"中来完成。Windows Server 2008 支持的网络服务虽然更多了,但默认不会安装任何组件,只是一个提供用户登录的、独立的网络服务器,用户可以根据自己的需要来安装相关的网络服务。

5.2.1　添加服务器角色

在 Windows Server 2008 中,所有的角色都可以通过"服务器管理器"添加。

(1) 在"服务器管理器"窗口中,单击"添加角色"链接,启动"添加角色向导",首先会显示图 5-1 所示的"开始之前"对话框,提示此向导可以完成的工作,以及操作之前应注意的相关事项。

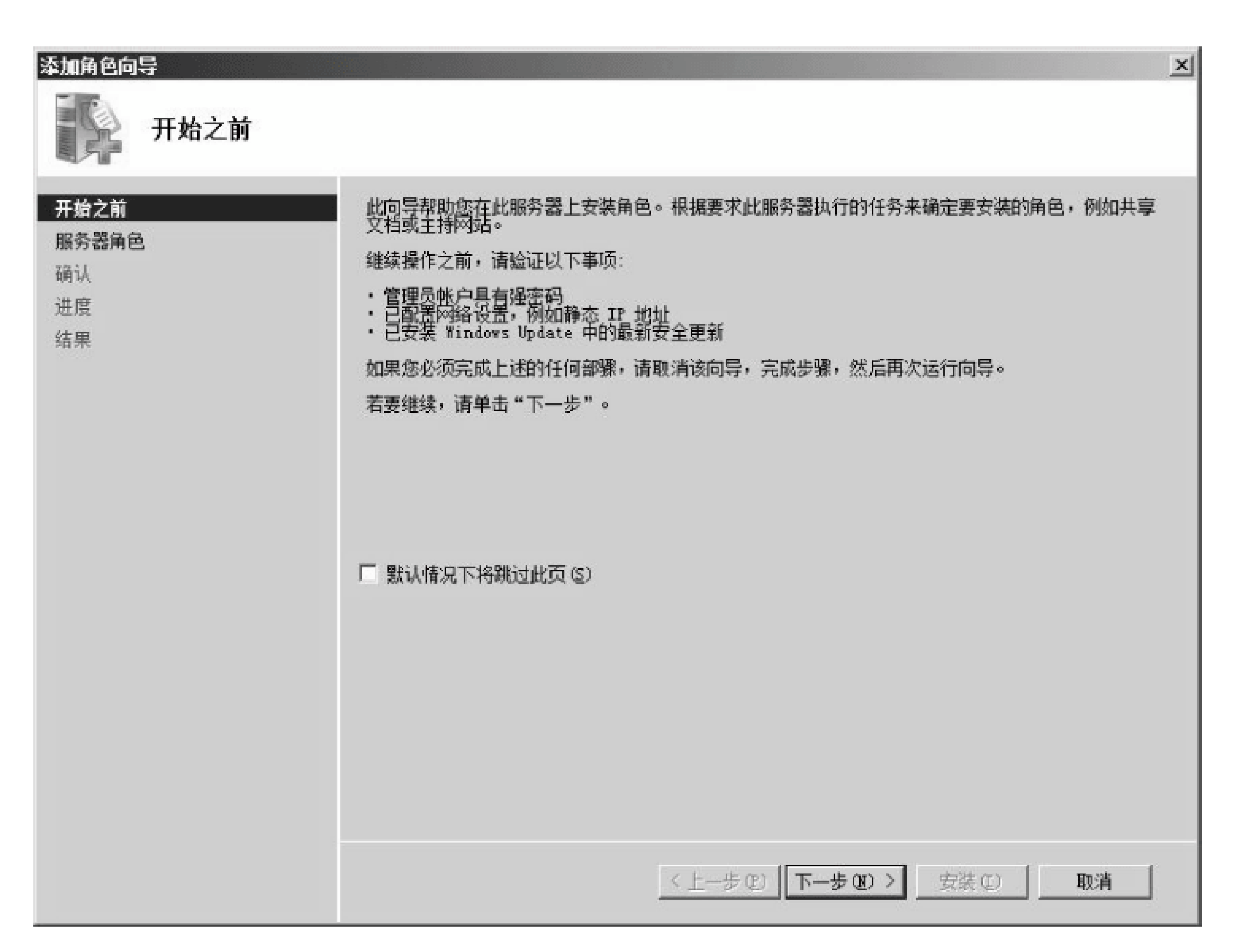


图 5-1　"开始之前"对话框

提示:如果完成"初始配置任务"后,阻止了该窗口开机时自动显示,则可以通过选择"开始"→"管理工具"→"服务器管理器"命令,打开"服务器管理器"窗口,展开"角色"目录,并单击右侧窗口中的"添加角色"链接,同样可以打开"添加角色向导"对话框。另外,

Windows Server 2008 安装完成后，默认会在快速启动栏中创建“服务器管理器”的快捷方式。

(2) 单击“下一步”按钮，显示图 5-2 所示的“选择服务器角色”对话框。所有可安装的网络服务全部显示在列表框中，Windows Server 2008 提供的服务器角色要比 Windows Server 2003 多了很多，这也是其功能强大的一个方面。如果角色前面的复选框是空的，则表示尚未安装，如果已选中，说明该网络服务已经安装。在列表框中选中拟安装的网络服务对应的复选框即可。



图 5-2 “选择服务器角色”对话框

注意：根据所选的服务器角色的不同，安装过程可能有所不同。

(3) 部分网络服务安装过程中可能需要提供 Windows Server 2008 安装光盘，按照提示操作即可。有些网络服务可能会在安装过程中调用配置向导，做一些简单的服务配置，但更详细的配置通常都借助于安装完成后的网络管理实现。

5.2.2 添加角色服务

服务器角色的模块化是 Windows Server 2008 的一个突出特点，不同的服务器角色可以完成独立网络功能。但是在安装某些角色时，同时还会安装一些扩展组件，来实现更强大的功能，普通用户完全可以根据自己的需要酌情选择。添加角色服务就是安装在先前安装过程中没有选择的子服务，例如“网络策略和访问服务”角色中包括的“网络策略服务器”、“路由和远程访问服务”、“健康注册机构”等，如果先前已经安装了“路由和远程访问服务”，则可按照如下操作步骤完成其他角色服务的添加。

(1) 依次选择“开始”→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口。在左侧栏中，依次展开“角色”→“Web 服务器(IIS)”目录，在右侧的“角色服务”区域中，即可查看所安装的功能组件，如图 5-3 所示。

(2) 单击“添加角色服务”链接，显示图 5-4 所示的“选择角色服务”对话框。在“角色服



图 5-3 查看角色服务组件

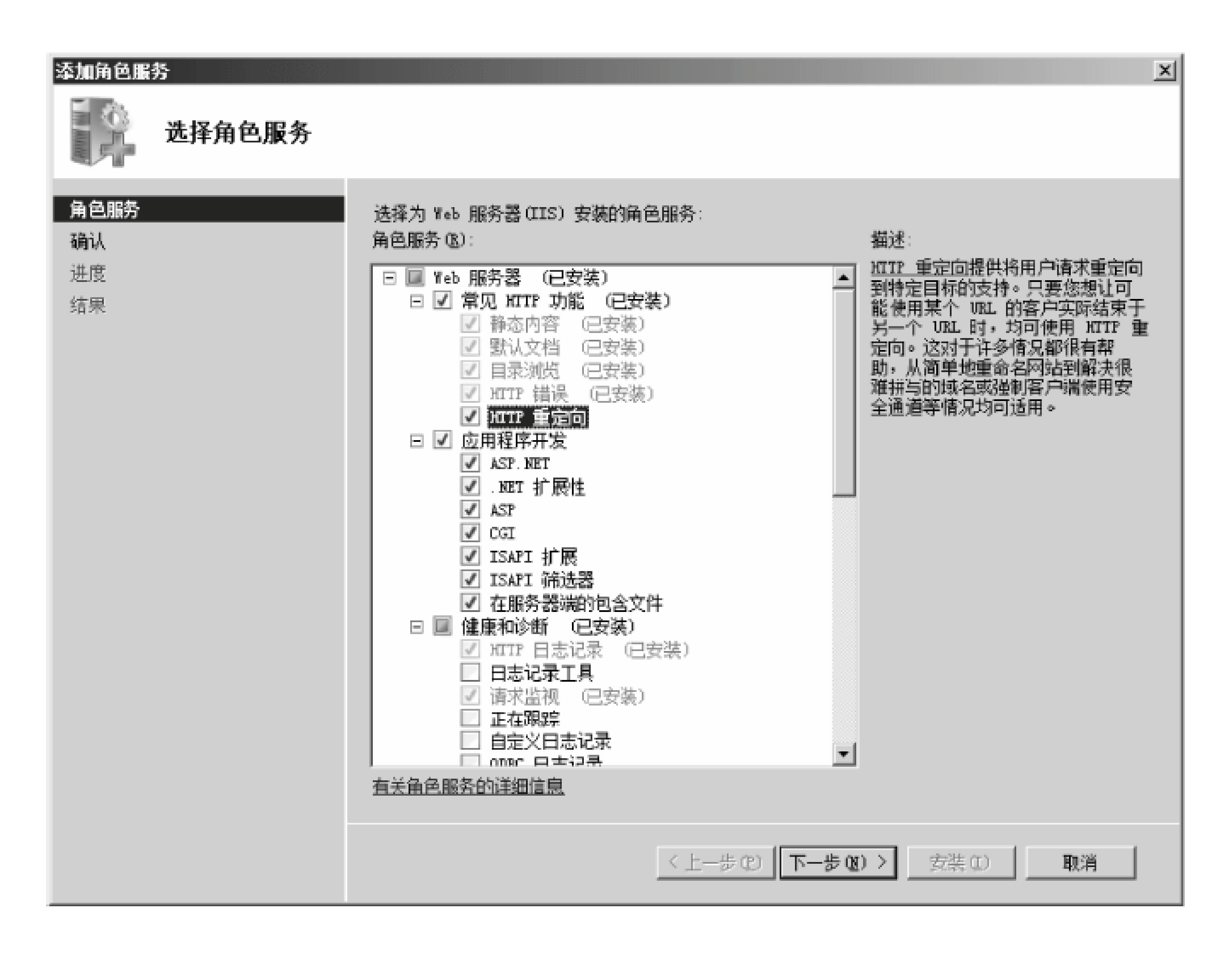


图 5-4 “选择角色服务”对话框

务”列表中,选中想要安装的角色服务的复选框。

(3) 单击“下一步”按钮,显示图 5-5 所示的“确认安装选择”对话框。检查所要安装的角色服务是否为想要的内容。

(4) 单击“安装”按钮,开始安装相应的角色服务。安装完成后,显示图 5-6 所示的“安装结果”对话框。

(5) 单击“关闭”按钮,关闭该向导即可。

5.2.3 删除服务器角色

服务器角色的删除同样可以在“服务器管理器”窗口中完成,需要注意的是,在删除角色



图 5-5 “确认安装选择”对话框



图 5-6 “安装结果”对话框

之前需确认是否有其他网络服务或 Windows 功能需要调用当前服务，以免删除之后造成服务器瘫痪。

（1）在“服务器管理器”窗口中，展开“角色”目录，会显示已经安装的服务角色，如图 5-7 所示。

（2）单击“删除角色”链接，打开图 5-8 所示的“删除服务器角色”对话框，取消选中想要删除的角色前的复选框，并单击“下一步”按钮，即可开始删除。

提示：角色服务的删除，同样需要在指定服务器角色的管理器窗口中完成，单击“角色服务”选项框旁边的“删除角色”链接即可。



图 5-7 已安装的服务角色

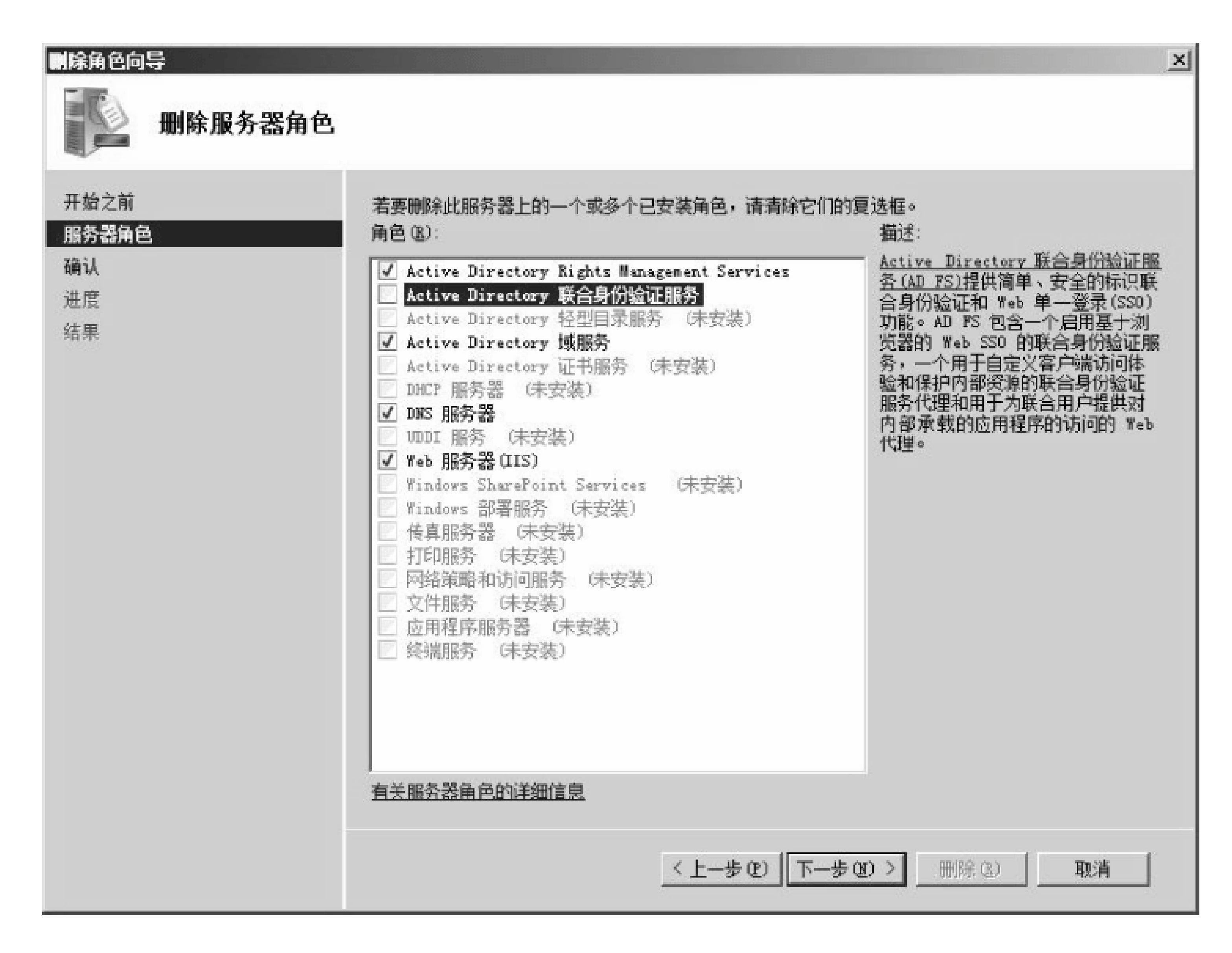


图 5-8 “删除服务器角色”对话框

5.3 网络服务管理控制台

通常情况下，网络服务的管理可以使用 MMC 控制台，或服务角色自身所提供的管理控制台进行管理。其中，使用 MMC 控制台可以实现在同一窗口中管理多个服务的目的，并且可以保存控制台文件，方便日后使用。而服务角色所提供的管理控制台，只能管理单一的服务类型，而不能像 MMC 控制台一样同时管理多种类型项目。

5.3.1 MMC 控制台统一管理

MMC 用于创建、保存并打开管理工具，以便使用这些管理工具来管理硬件、软件和 Windows 系统的网络组件。MMC 可以运行于各种 Windows 9x 和 Windows NT 操作系统上，以及 Windows XP Home Edition、Windows XP Professional、Windows Server 2003 和 Windows Server 2008 家族的操作系统上。

1. MMC 控制台

在 Windows 2000 以前版本中的管理工具都是一些可执行的程序，只能在安装了相应产品的计算机上执行相应的管理功能。Windows 2000 及以后的应用程序(如 Microsoft Exchange、Microsoft ISA Server、Windows XP 等)都支持 MMC。

使用 MMC，除了有统一的、标准的管理界面之外，还可以在一个 MMC 的管理界面中管理所有的、本地的或远程的计算机上的相应信息。图 5-9 所示为包括了常用管理程序的 MMC 的管理界面。



图 5-9 集成了常用管理工具的 MMC

MMC 有着统一的管理界面，MMC 控制台由 3 个窗格组成。左边窗格显示控制台树，控制台树显示控制台中可以使用的项目；中间的窗格为详细信息窗格，详细列出这些项目的信息和有关功能，随着单击控制台树中的不同项目，详细信息窗格中的信息也将变化，详细信息窗格可以显示不同的信息，包括网页、图形、图表、表格和列，当选中某个项目时，在右侧窗格中可以对该项目进行相应的操作。

每个控制台都有自己的菜单和工具栏，与主 MMC 窗口的菜单和工具栏分开，这有利于用户执行任务。Windows Server 2008 系统的 MMC 控制台版本为 3.0，如图 5-10 所示。

2. MMC 控制台的使用

使用 MMC 控制台，可以管理本地计算机或远程计算机的一些服务或应用，这些与安装在要管理的计算机上的程序相关，例如，想管理一台计算机的磁盘，可以在 MMC 控制台中添加磁盘管理单元，具体操作步骤如下。

(1) 依次选择“开始”→“运行”命令，打开“运行”对话框，在“打开”文本框中输入 mmc，

如图 5-11 所示。



图 5-10　控制台版本



图 5-11　“运行”对话框

(2) 单击“确定”按钮，显示 MMC 管理控制台。

(3) 依次选择“文件”→“添加/删除管理单元”命令，或者按 Ctrl＋M 键，显示图 5-12 所示的“添加或删除管理单元”对话框。



图 5-12　“添加或删除管理单元”对话框

(4) 在左侧“可用的管理单元”列表中，选择欲添加的管理单元，单击“添加”按钮，添加管理单元。如果添加的管理单元只能管理本地计算机，管理插件会自动添加到 MMC 控制台中，如果添加的插件也可以管理远程计算机时，则会显示相应的选择界面。这里以添加“计算机管理”为例进行介绍，显示图 5-13 所示的“计算机管理”对话框。在该对话框中，可以设置是管理本地计算机，还是管理远程计算机，如果选中“本地计算机(运行这个控制台的计算机)”单选按钮，则可以添加管理本地计算机的管理单

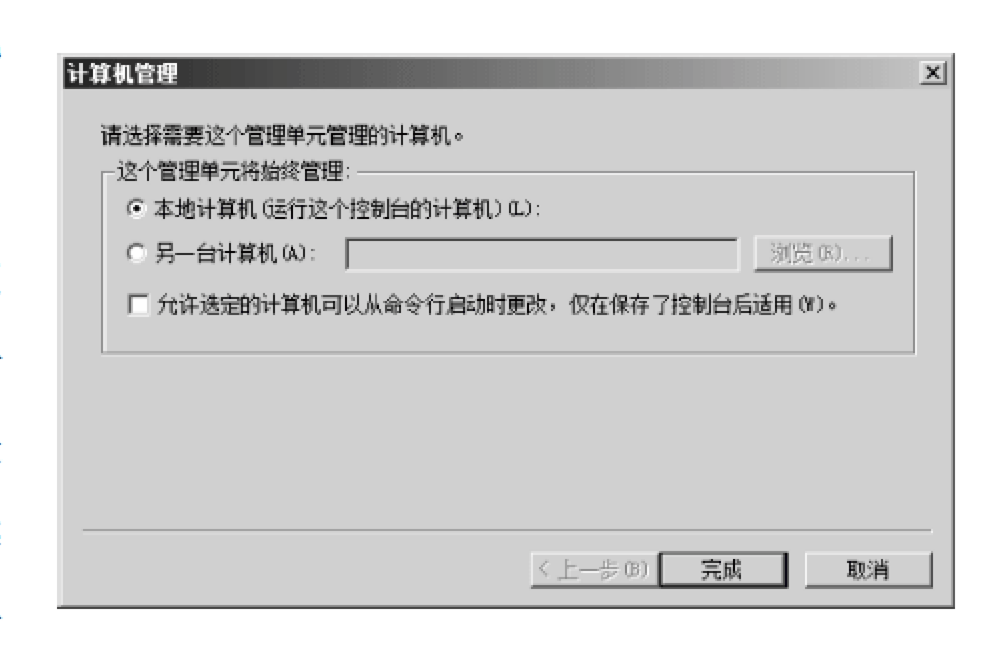


图 5-13　“计算机管理”对话框

元，如果选中“另一台计算机”单选按钮，并输入远程计算机的名称，可管理远程计算机。这里选中“本地计算机”单选按钮。

（5）单击“完成”按钮，即可将该管理单元添加到右侧“所选管理单元”列表中，如图 5-14 所示。重复操作，可添加多个管理单元。

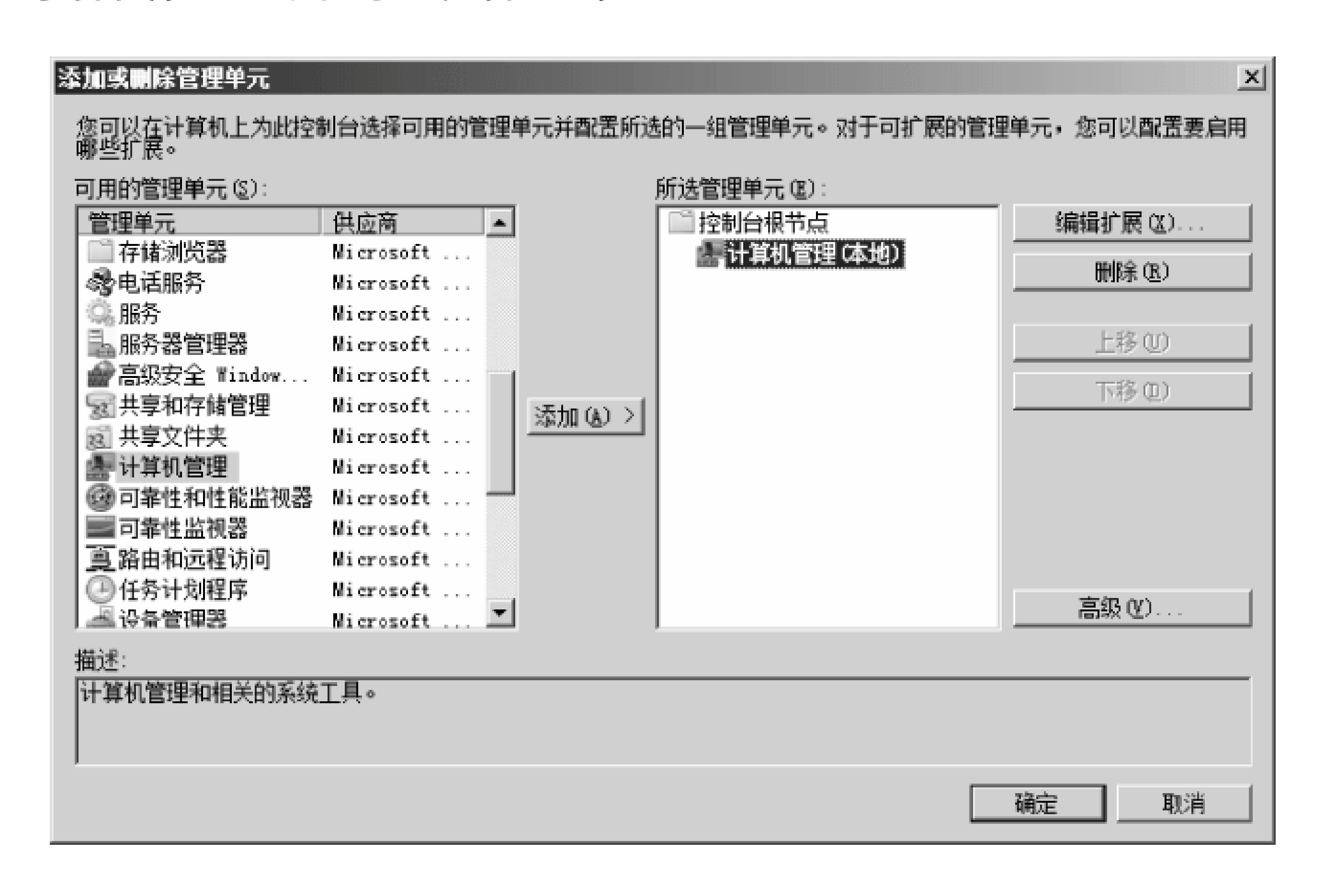


图 5-14　完成管理单元添加

（6）单击“确定”按钮，完成并关闭“添加或删除管理单元”对话框，返回 MMC 控制台，成功添加相应的管理单元，如图 5-15 所示。



图 5-15　添加完管理插件的 MMC 控制台

5.3.2　独立管理控制台

针对于不同的网络服务，微软定制了特定的管理控制台，不同的管理控制台只能管理特定的角色，例如“Active Directory 用户和计算机”管理控制台，只能管理与域用户和计算机相关的功能和设置，如图 5-16 所示。



图 5-16 “Active Directory 用户和计算机”管理控制台

5.4 网络服务状态监控

操作系统是整个服务器提供服务的基础，如果操作系统发生故障，则不能为网络提供服务。通过使用系统管理工具，可以时刻监视远程服务器或计算机的操作，例如监视远程服务器的网络服务运行情况、远程计算机的运行状态、检查远程计算机的计算机属性设置等。

5.4.1 网络服务监视器——Servers Alive

Servers Alive 的主要功能为监控远程服务器上所运行的各种服务的状态，是一款功能强大的监控软件。当服务器出现问题时，可以使用多种方式报警，例如发生声音、发送 E-mail 等。该软件的安装比较简单，只需保持默认设置即可，这里就不再赘述。需要注意的是，在软件安装完成后，需要重新启动计算机才能使软件正常工作。

1. 设置监控服务

(1) 依次选择“开始”→“程序”→Alive→Servers Alive 命令，显示图 5-17 所示的 Servers Alive 主界面。

(2) 添加需要监控的内容。单击 Add 按钮，显示图 5-18 所示的 Entries 对话框。

General 选项卡中部分参数的含义如下。

① Server name or IP[X] address：要监控的服务器的主机名或 IP 地址。

② Pretty name：项目名称。该名称只是为了与其他项目相区分，并无实际意义。

③ Host ID：要在 Servers Alive 中显示的顺序数值，也可由程序根据添加项目的先后顺序自动设置。



图 5-17 Servers Alive 主界面

④ Remark：设置项目的备注信息。

⑤ Active/Maintenance：选择该项目是 Active(活动)或 Maintenance(维护)。

(3) 选择图 5-19 所示的 Check 选项卡，设置检测项目。在 Check to use 下拉列表框中可选择要监控的项目，如 Ping、各种服务(NT service)、进程(NT prosess)、硬盘空间(Diskspace)、URL、数据库(Database)、External COM 等，例如，要监控服务器上的 FTP 服务，可选择 TCP Protocol 选项，然后在下面的列表框中选择 FTP 选项，在 on port 选项区域中会自动显示选中默认端口 Default(21)单选按钮，如果 FTP 服务使用的不是 21 端口，可在 other 文本框中输入相应的端口号。

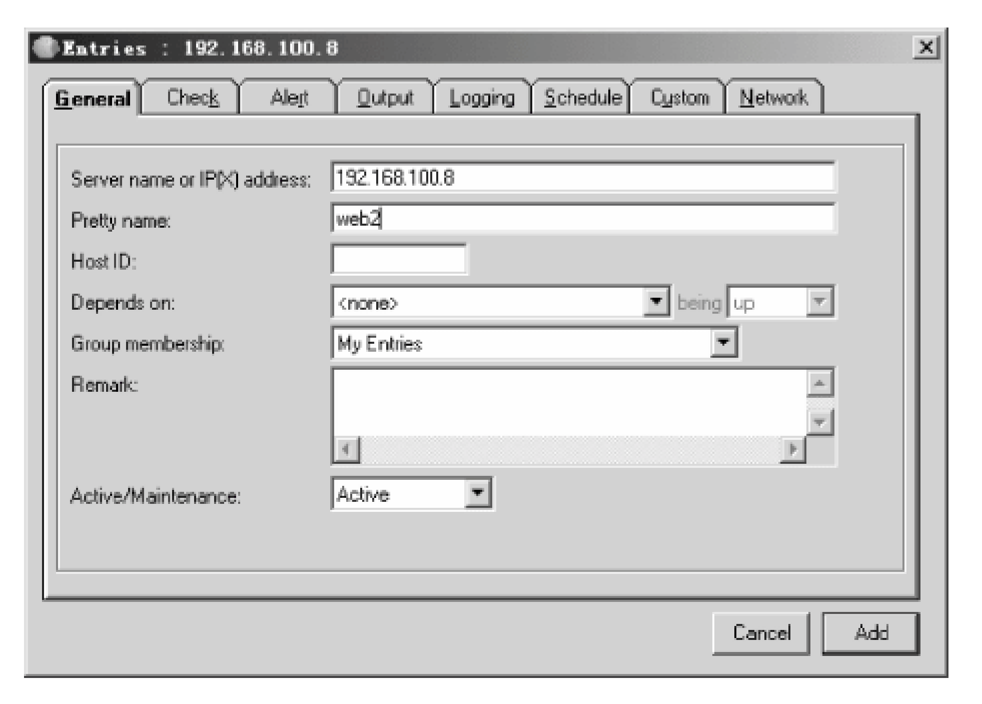




图 5-18 General 选项卡

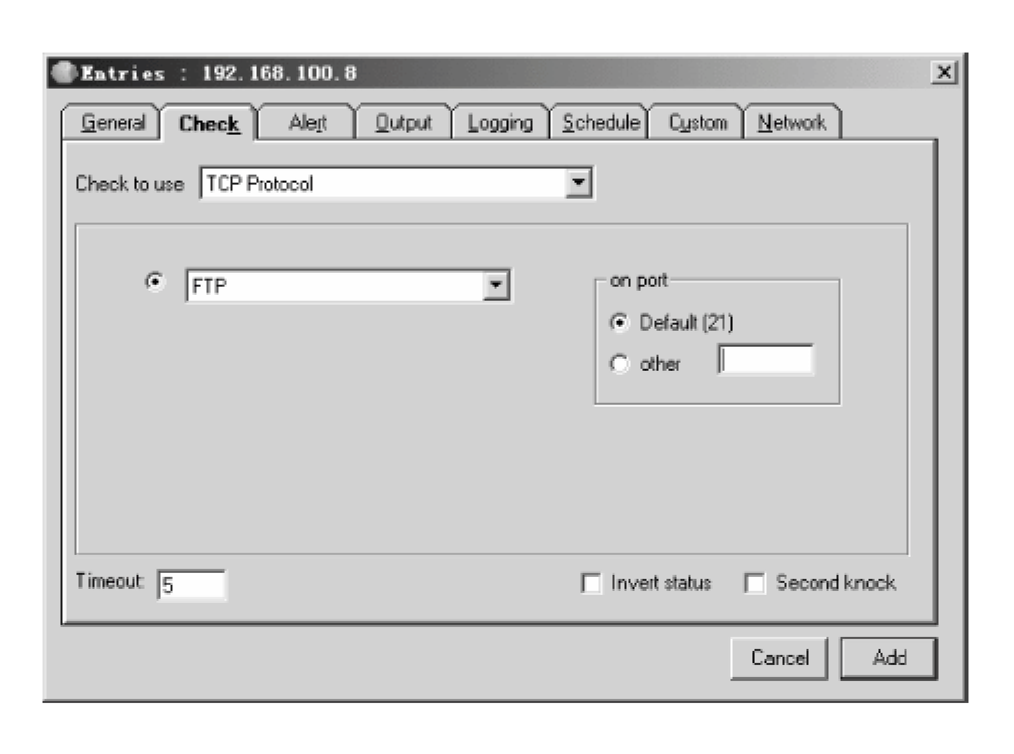


图 5-19 Check 选项卡

(4) 选择 Alert 选项卡，设置警报方式。单击 Add 按钮，显示图 5-20 所示的快捷菜单，Servers Alive 提供了多种警报方式，如发送邮件(Send SMTP mail)、声音报警(Sound)、发送 ICQ/MSN/MIM/WinPOPUP 消息等，根据需要进行设置即可。

① 这里以发送邮件警报为例。在 Add 快捷菜单中选择 Send SMTP mail(primary)命令，显示图 5-21 所示的 Add/edit alert 对话框。默认显示 What 选项卡，在 To 文本框中输入要接收报警邮件的邮箱地址，在 Subject 文本框中设置邮件主题，在 Message(body)文本框中设置要发送的内容，这里使用不同符号代替，如%p 表示 IP 地址等，也可以使用文本信息。

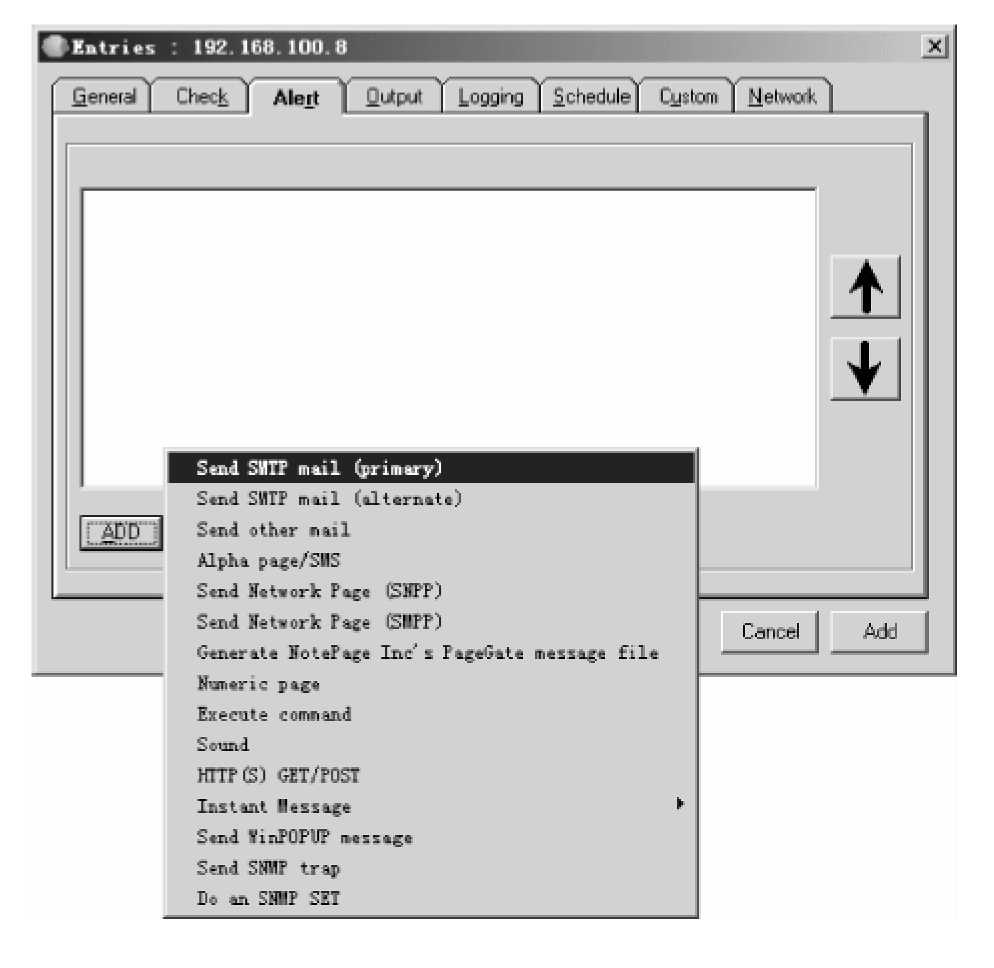


图 5-20 添加警报方式

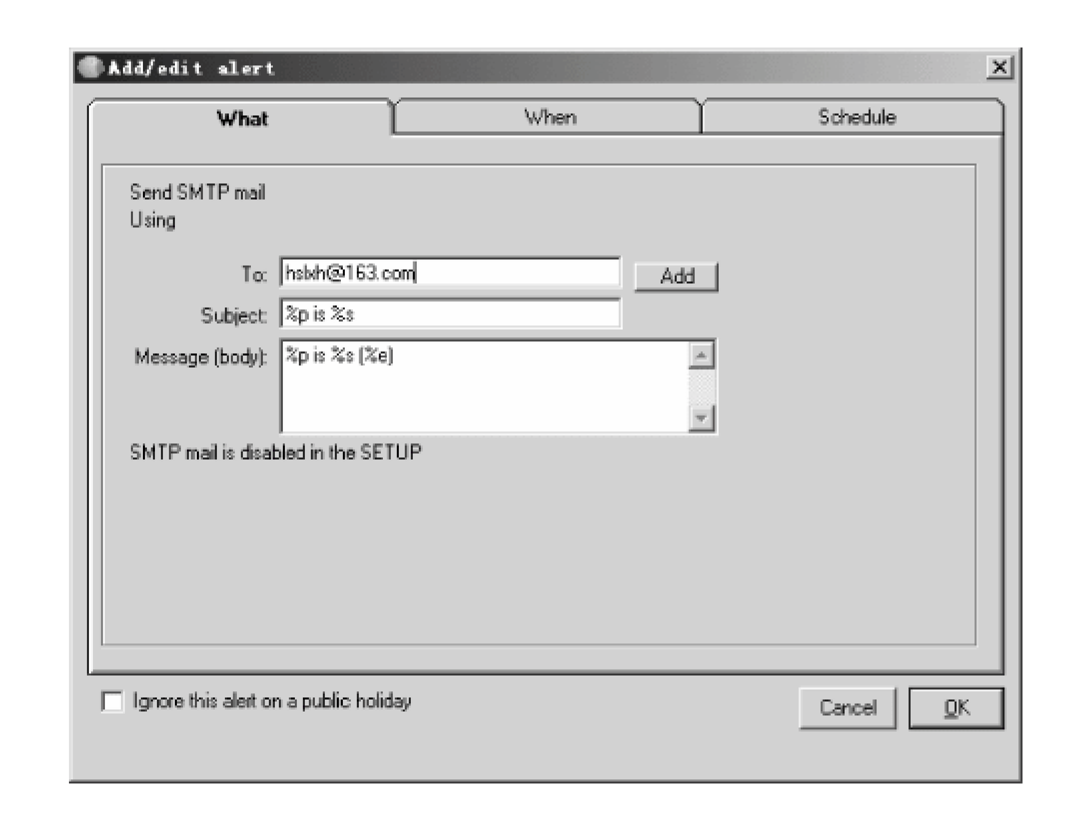


图 5-21 What 选项卡

② 选择 When 选项卡，根据用户实际需要设置发送报警的条件，如图 5-22 所示。

③ 选择 Schedule 选项卡，设置发出警报的时间，默认在任意时间都可以使用警报。如果需要在某段时间不发出警报，例如在周六和周日不发出警报，需选中 Use alert schedule 复选框，然后在其选项区域中选中 Saturday 和 Sunday 区域，单击 Don't Alert 按钮，该区域就会变成红色，表示在该时间段内不使用警报，如图 5-23 所示。其中，绿色方块表示使用警报，红色方块表示不使用警报。

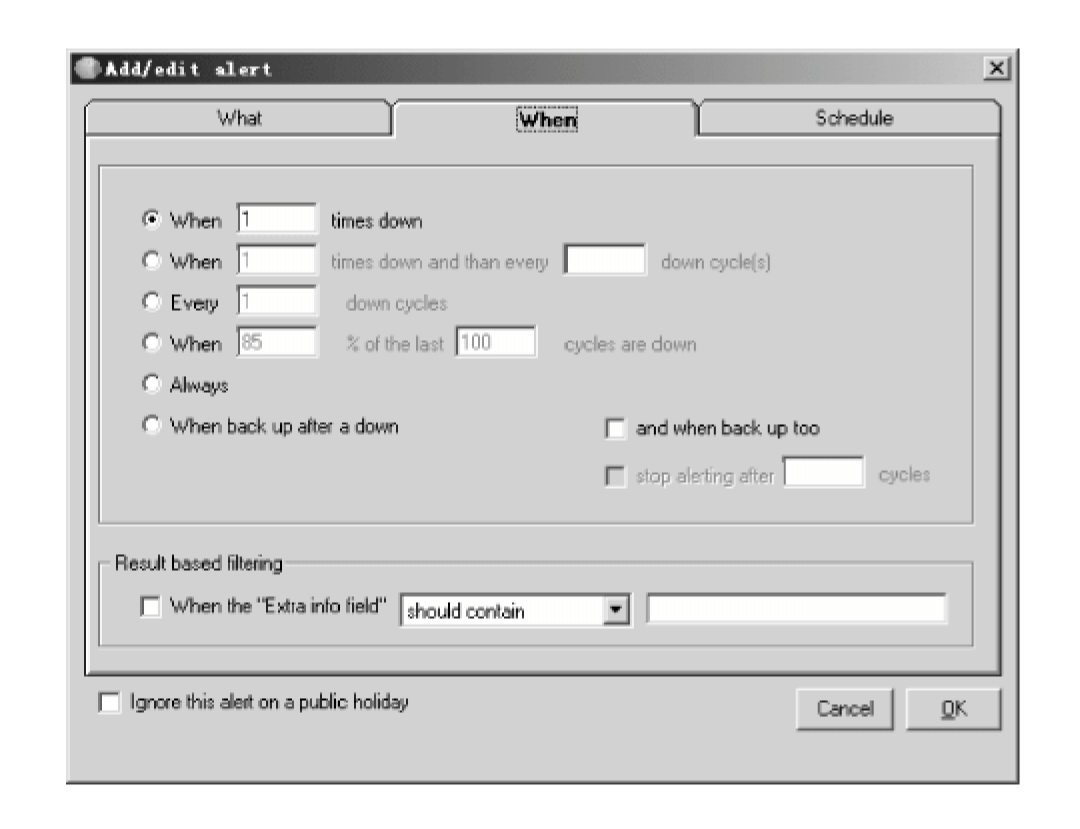


图 5-22　When 选项卡

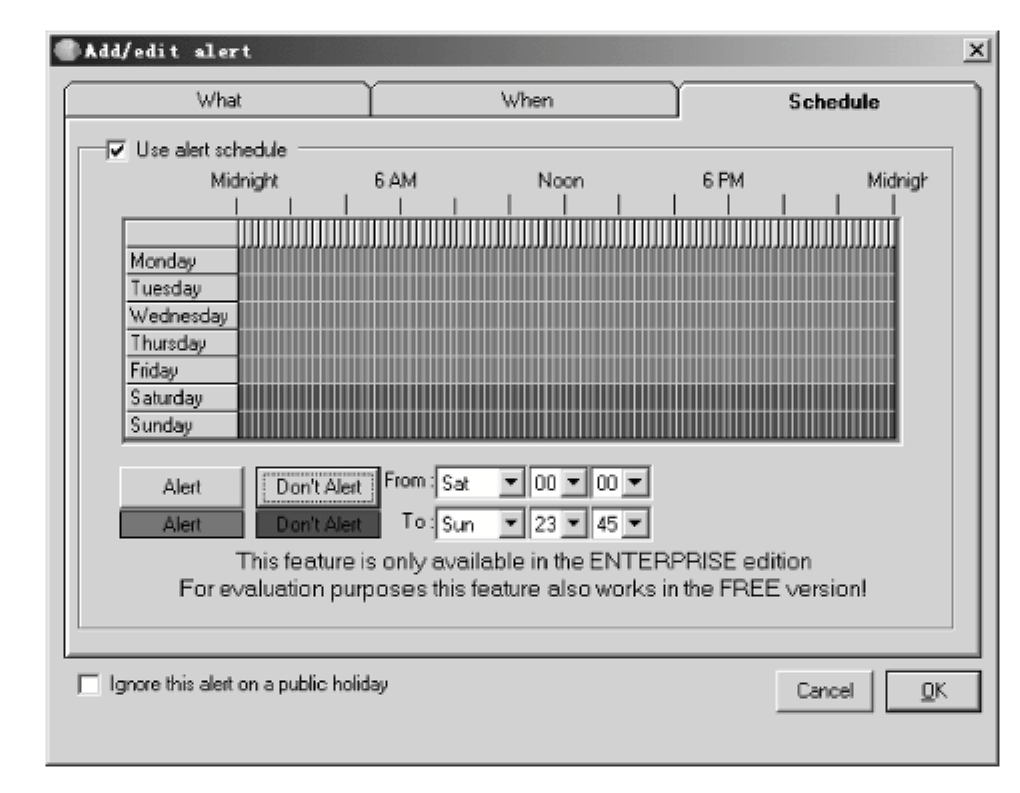


图 5-23　Schedule 选项卡

④ 设置完成以后，单击 OK 按钮，该警报即可添加到 Entries 对话框中的 Alert 列表中。重复操作，可以添加多种方式的报警。如果添加了多种报警方式，可以通过单击↑和↓按钮设置报警顺序。

(5) 为了方便管理员查看警报的结果，可以将结果输出为网页形式。选择 Output 选项卡，单击 Add 按钮，显示 Add HTML page 对话框，可添加一个 HTML 页，如图 5-24 所示。

(6) 选择 Logging 选项卡，设置要记录的日志类型，如图 5-25 所示。Servers Alive 可以将每次的运行状况记录到监控日志中。

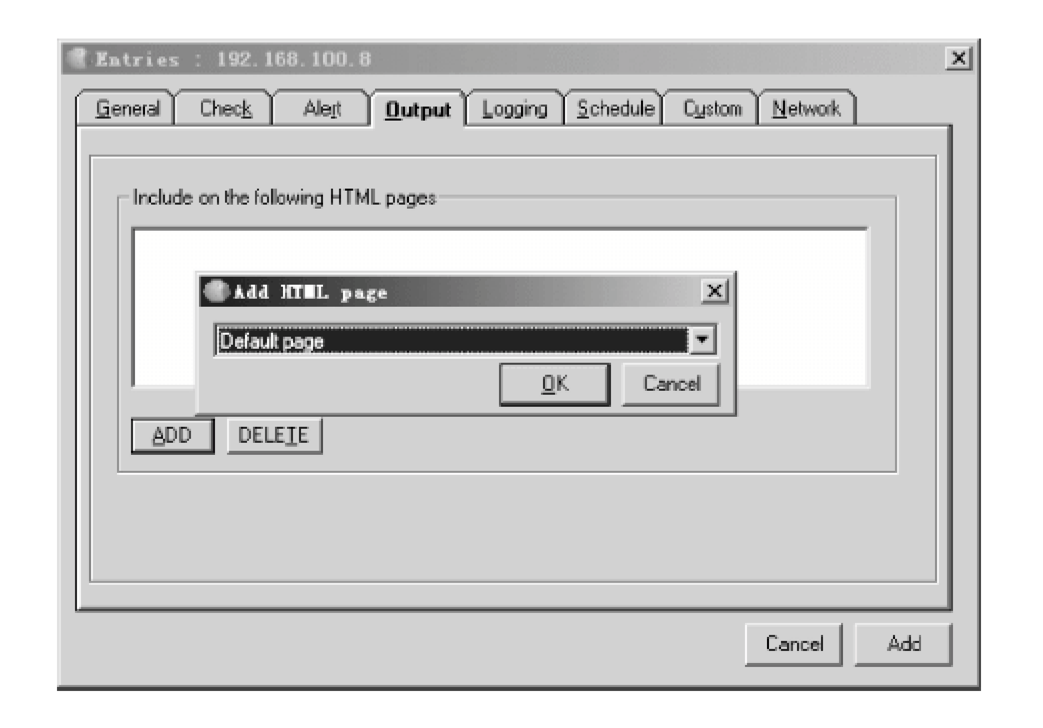


图 5-24　Add HTML page 对话框

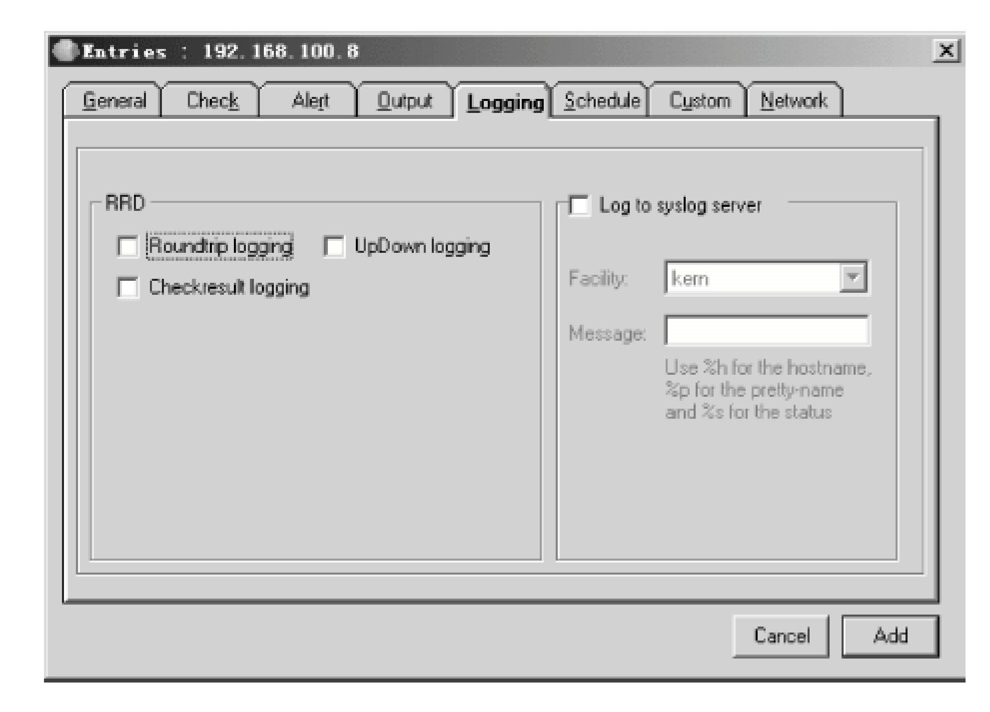


图 5-25　设置日志

(7) 选择 Schedule 选项卡，设置监控时间表，如图 5-26 所示。默认每天 24 小时都会自动监测，如果想让某个时间段不进行监测，可选中相应的时间段，并单击 Don't check 按钮即可。

(8) 最后单击 Add 按钮，该监控服务便会添加到 Servers Alive 窗口中。重复操作，可

以添加多个监控服务，如图 5-27 所示。

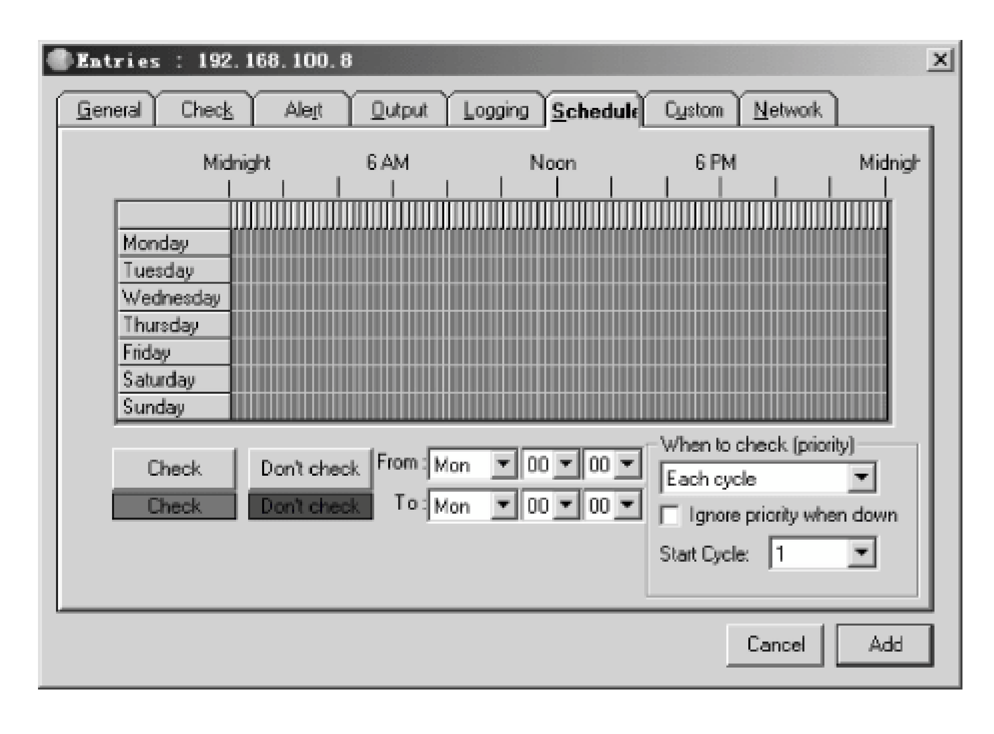


图 5-26　设置监控时间表

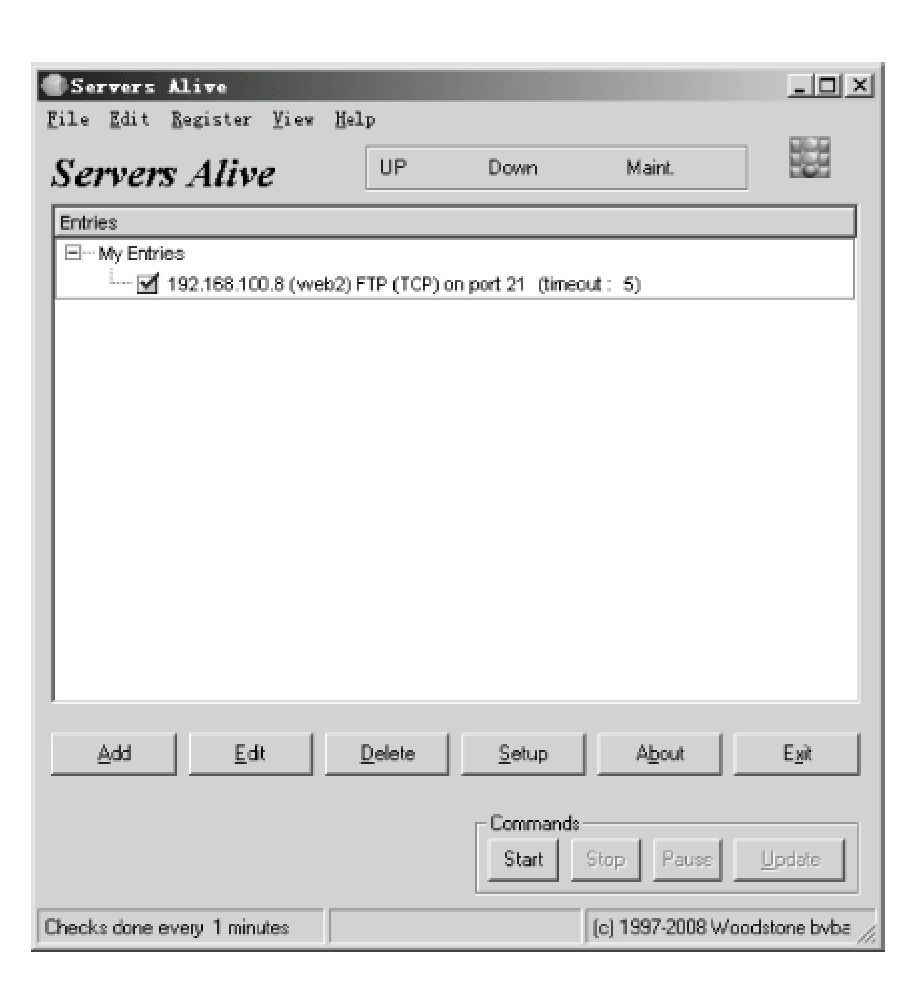


图 5-27　监控内容

（9）单击 Commands 选项区域的 Start 按钮，Servers Alive 即可开始进行监控，并且每隔 5 分钟检测一次，监测结果会显示在主窗口上方。单击 Update 按钮可立即更新。

选中某个监控的项目，单击 Edit 按钮可编辑该项目；单击 Setup 按钮可设置 Servers Alive；单击 About 按钮显示 Servers Alive 的版本等信息；单击 Exit 按钮退出 Servers Alive。默认会监控所有添加的服务，如果不想监控某项服务，只要取消该服务相应的复选框即可。

2. 设置邮件警报

在 Servers Alive 中，使用电子邮件可以向管理员发送警报，使管理员及时了解到所监控的服务所发生的变化，这也是使用该软件最常用的报警方式。

（1）在 Servers Alive 主窗口中，单击 Setup 按钮，显示 SETUP 对话框，展开 Alerts→SMTP 目录，即可设置邮件警报。这里以 Primary 为例进行介绍，如图 5-28 所示，选中 Enable primary SMTP mail 复选框，在 Mail host 文本框中输入发送邮件服务器（SMTP 服

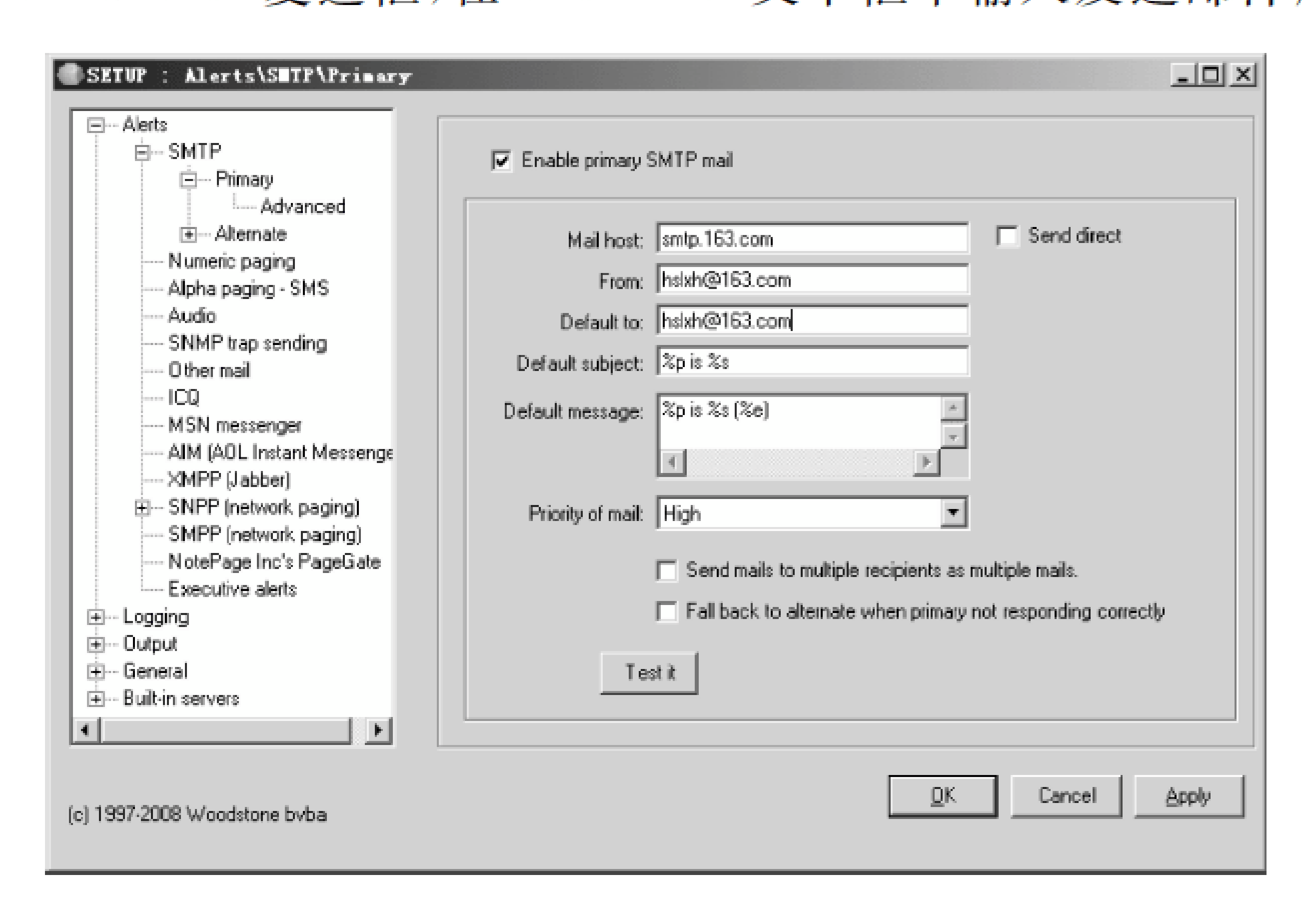


图 5-28　设置邮件警报

务器)地址;在 From 文本框中输入用来发送邮件的邮箱,在 Default to 文本框中输入接收邮件的邮箱,在 Default subject 和 Default message 文本框中分别输入邮件主题和内容。最后单击 Apply 按钮应用设置即可。

(2) 选择 Advanced 选项,如图 5-29 所示。如果选中 Use SSL 复选框,可以使用 SSL 方式进行连接。在 Authentication 下拉列表框中选择 ESMTP 选项,并在 Username 和 Password 文本框中分别输入邮箱的登录名和密码,最后单击 OK 或 Apply 按钮应用修改。

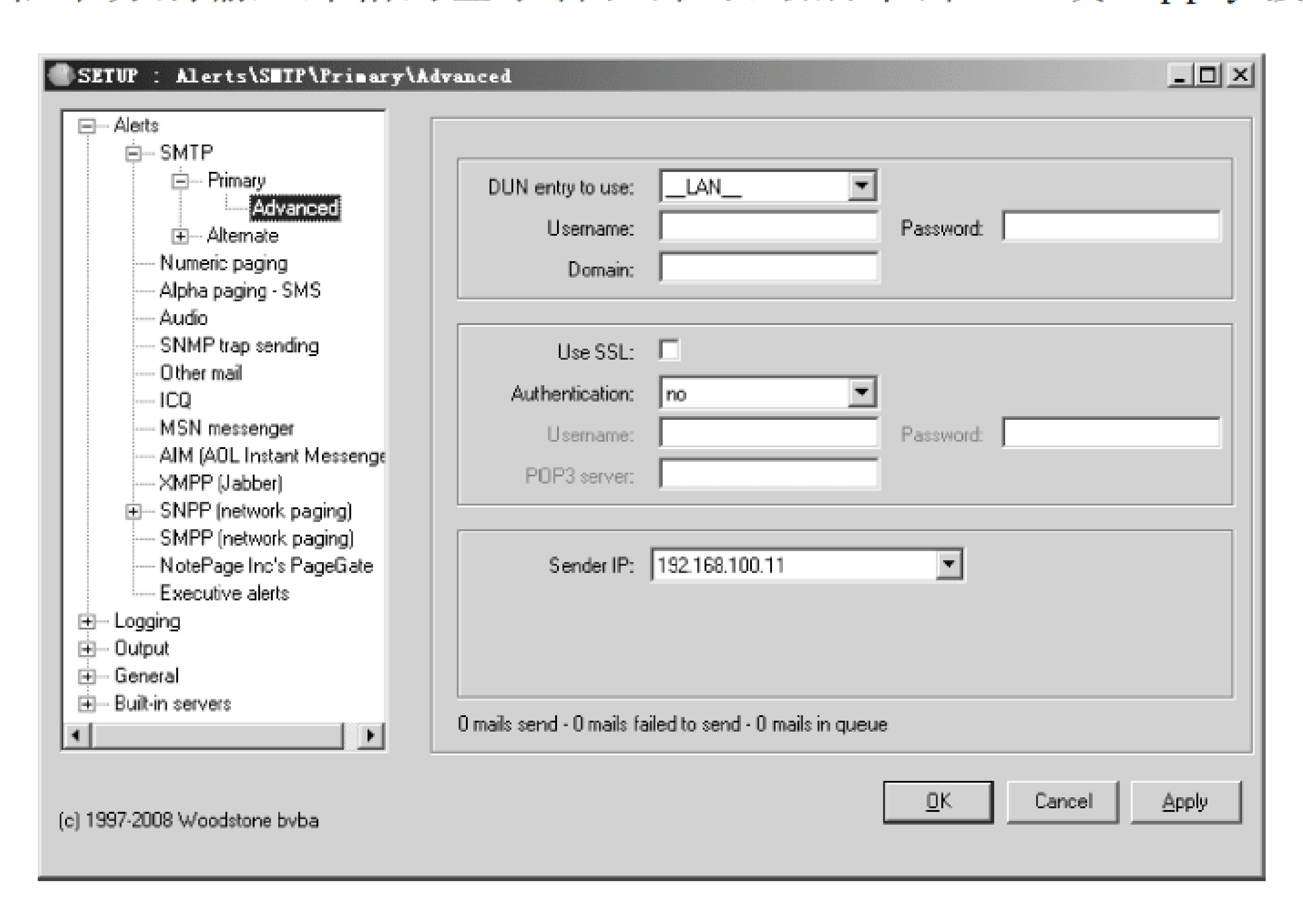


图 5-29 设置邮箱登录名和密码

(3) 设置完成以后,可以测试一下邮件警报是否有效。在 Primary 窗口中单击 Testit 按钮进行发送邮件测试,如果所设置的接收邮箱中能收到测试邮件,说明邮件警报设置正常,否则就需要检查并重新设置。按照上述同样设置,也可以在 Alternate 中设置发送邮件警报服务器。

(4) 单击 OK 按钮。此时,当 Servers Alive 在检测到警报时就会使用所设置的邮箱来发送邮件。

3. 查看监控状态

Servers Alive 内置有 Web Server、Telnet Server、SSH Server、SNMP Trap Receiver 等几种服务,通过 Servers Alive 可以查看这几种服务的活动状态。这里以 Web Server 为例进行介绍。

在 Servers Alive 主窗口中,单击 Setup 按钮,显示图 5-30 所示的 SETUP 窗口,依次展开 Built-in servers→Web server 目录,选中 Enable web server[HTTP]复选框,在 Web server port number 文本框中设置 Web 服务的端口,默认为 4310 端口;选中 Enable automatic web page update 复选框以自动更新网页内容。

最后,单击 Apply 或 OK 按钮保存并应用设置即可。

在网络中任何一台可以连接到监控服务器的计算机上,在 IE 浏览器地址栏中输入如下格式内容:http://IP 地址或主机名:4310/status,按 Enter 键确认,即可查看 Servers Alive 监控的内容,包括所监控的项目及最后一次检测的时间,如图 5-31 所示。

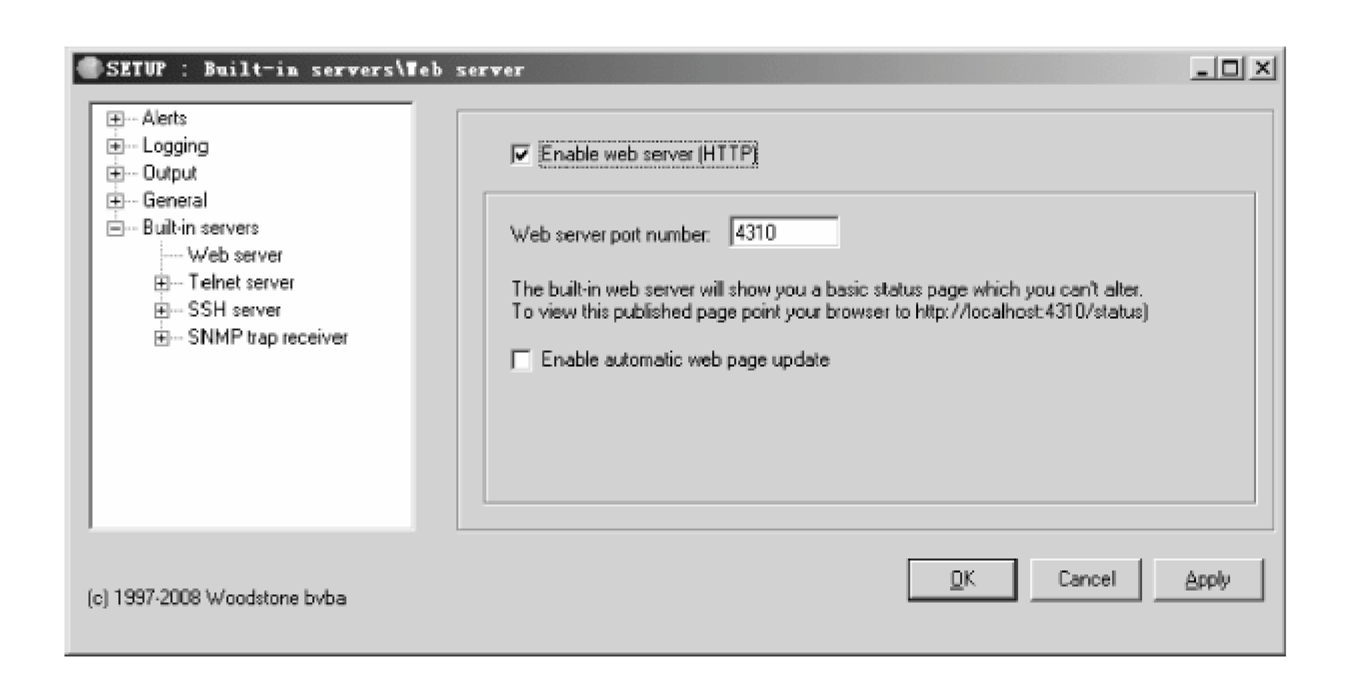


图 5-30 设置 Web Server

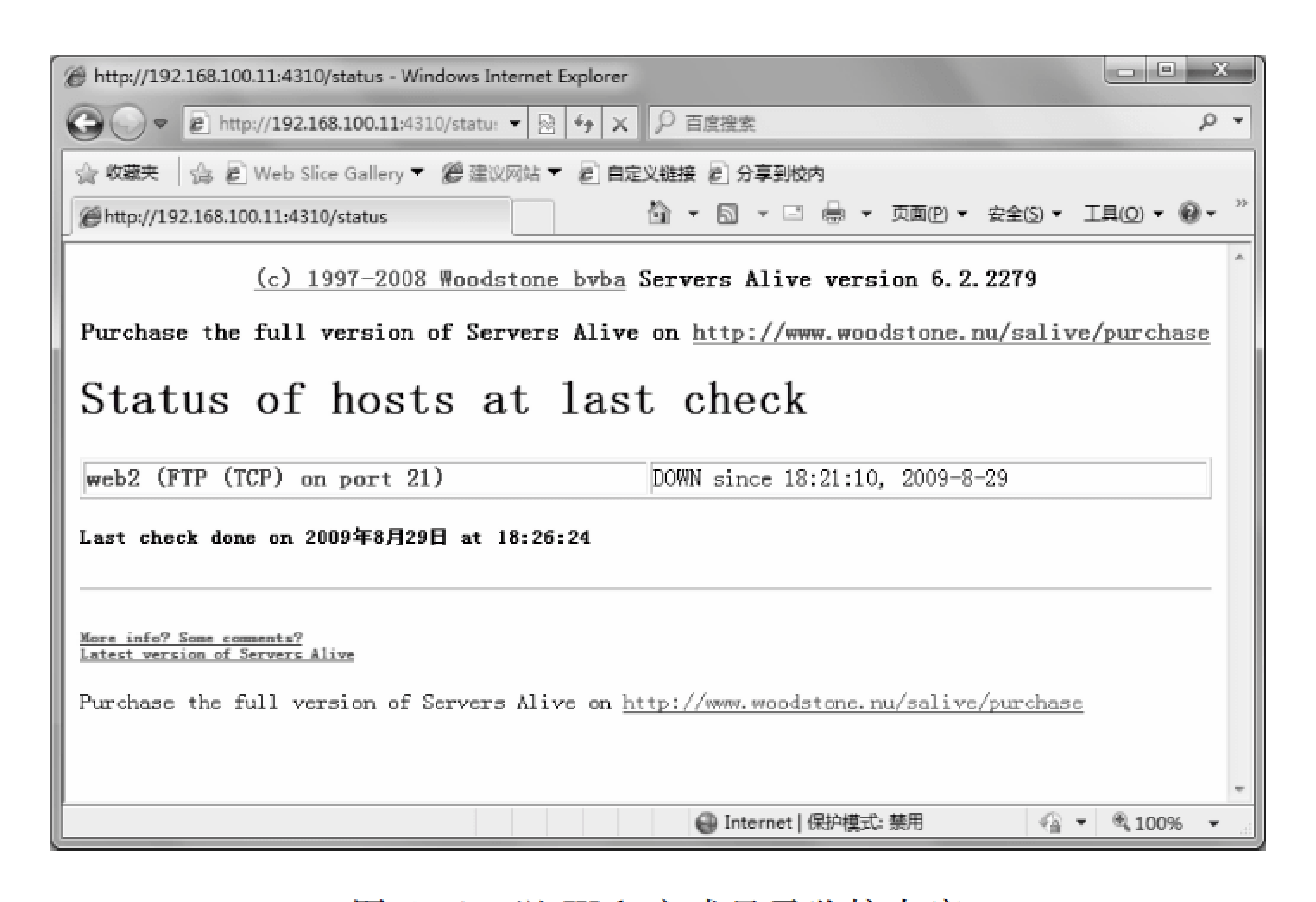


图 5-31 以 Web 方式显示监控内容

5.4.2 OpManager 监视 Windows 服务

OpManager 是一款专业有效的网络和应用管理软件，包含 WAN 监控、服务器管理、系统和应用程序、网络性能分析和报表管理等功能。OpManager 具有操作简单的优点，可以实现网络和数据中心监控能力，从而使复杂的 IT 管理简单易行。该软件可以在其官方网站（www.adventnet.com.cn）上进行下载。

1. 启用 SNMP

不但网络设备可以通过启用 SNMP 字符串功能进行管理，网络中的服务器同样可以通过启动 SNMP 进行管理。但无论是 Windows Server 2003 还是 Windows Server 2008，必须首先安装简单网络管理协议（SNMP），在安装完成后其设置操作基本相同。这里以 Windows Server 2003 为例介绍简单网络管理协议的安装与设置。

（1）依次选择“开始”→“控制面板”→“添加或删除程序”命令，打开“添加或删除程序”窗口。然后在左侧栏中单击“添加/删除 Windows 组件”按钮，打开“Windows 组件向导”对话框，在“组件”列表中选中“管理和监视工具”复选框，然后单击“详细信息”按钮，显示图 5-32 所示的“管理和监视工具”对话框。在“管理和监视工具 的子组件”列表中，选中“简单网络管理协议（SNMP）”复选框。



图 5-32　“管理和监视工具”对话框

(2) 单击“确定”按钮，返回“Windows 组件向导”对话框。然后单击“下一步”按钮，即可开始安装简单网络管理协议(SNMP)，并根据提示插入 Windows Server 2003 安装光盘。安装完成后，单击“完成”按钮，完成并关闭向导即可。

(3) 依次选择“开始”→“管理工具”→“服务”命令，打开“服务”窗口。在服务列表中，双击 SNMP Service 选项，打开“SNMP Service 的属性(本地计算机)”对话框。选择图 5-33 所示的“安全”选项卡，如果网络中设置有 SNMP 陷阱，可以选中“发送身份验证陷阱”复选框，并进行相关的设置，这里取消选中该复选框。

(4) 单击“添加”按钮，显示图 5-34 所示的“SNMP 服务配置”对话框。在“团体权限”下拉列表框中，选择想要添加的 SNMP 字符串的权限，在“团体名称”文本框中，输入所使用的 SNMP 字符串。重复操作，可添加多个权限不同的 SNMP 字符串。

(5) 根据需要选择接受 SNMP 数据包的方式，这里选中“接受来自这些主机的 SNMP 数据包”单选按钮。默认会自动创建一个接受本地计算机的列表项，选择该选项并单击“编辑”按钮，显示图 5-35 所示的“SNMP 服务配置”对话框。在“主机名，IP 或 IPX 地址”文本框中，输入指定的服务器的信息。

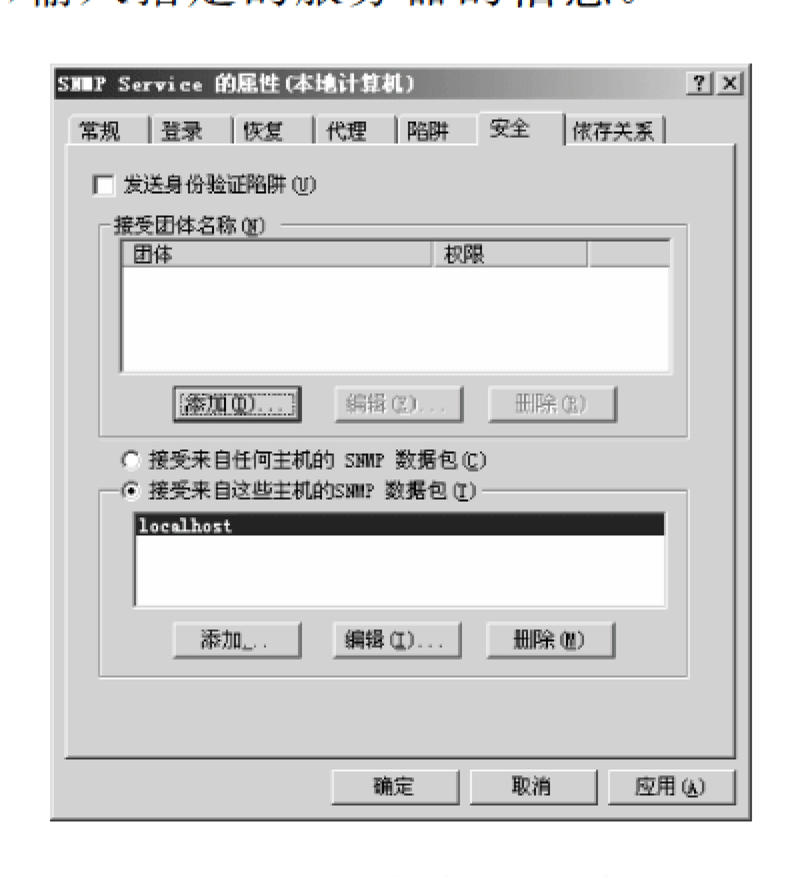


图 5-33　“安全”选项卡



图 5-34　“SNMP 服务配置”对话框

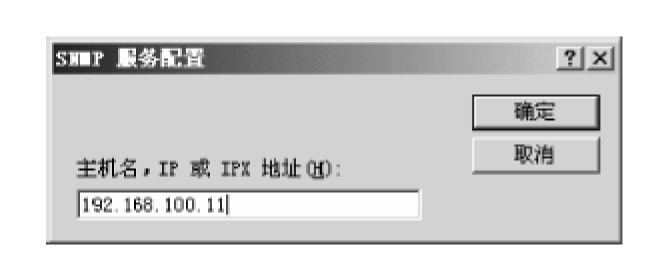


图 5-35　设置接受 SNMP 数据包的方式

(6) 依次单击“确定”按钮，保存设置即可。

对于 Windows 2008 服务器，在“服务器管理器”窗口的左侧栏中展开“功能”目录，在右侧栏中单击“添加功能”功能按钮，显示图 5-36 所示的“选择功能”对话框。在“功能”列表中，选中“SNMP 服务”复选框。单击“下一步”按钮，根据提示完成安装操作即可。



图 5-36 “选择功能”对话框

安装完成后，具体设置 SNMP 服务的操作，与 Windows 2003 相同，这里就不再赘述。

2. 安装 OpManager

OpManager 是 AdventNet 所提供的一款管理网络、系统及应用程序的工具，适用于 Windows、Linux、Solaris 等多种系统。OpManager 具有故障、性能报表，资源清单管理，全面支持 SNMP 协议，监控包括数据库、Web、FTP、邮件服务器等功能。

(1) 系统需求

安装 OpManager 的系统需求如表 5-1 所示。

表 5-1 安装 OpManager 的系统需求

设备数量	处理器主频	内 存	硬 盘	操作系统
50 以下	1.7GHz	1GB	20GB 空闲空间	Windows：Windows Server 2003，Windows 2000 Professional＋SP4，Windows XP Professional Linux：Red Hat 7.x 以上，Debian 3.0
50～150	2.4GHz	2GB		
150～300	3.4GHz	2GB		
300～500	2×3.4GHz	4GB		
500 以上	4×3.4GHz	4GB		

(2) OpManager 安装

OpManager 软件包可以从 AdventNet 的官方网站(http://www.adventnet.com.cn)下载得到，目前 OpManager 软件包的最新版本为 OpManager 7.0。主要操作步骤如下。

在图 5-37 所示的 Web Server Port 对话框中，设置 OpManager 的服务器运行端口，默认服务器端口为 80。如果当前系统上运行有其他的 Web 服务器(例如 IIS)，为了避免端口

发生冲突，建议在安装时，选择一个 80 以外的不常用的端口(例如 9090、9088 等)，这里使用 9088 端口。

在图 5-38 所示的 Select the backend database for OpManager 对话框中，如果选中 MySQL (Bundled with the Product)单选按钮，可以在安装 OpManager 的同时，安装软件所需要的数据库软件。如果选中 MSSQL 单选按钮，可以让 OpManager 使用网络中的 SQL Server 2000 或 SQL Server 2005 数据库。这里选中 MySQL(Bundled with the Product)单选按钮。

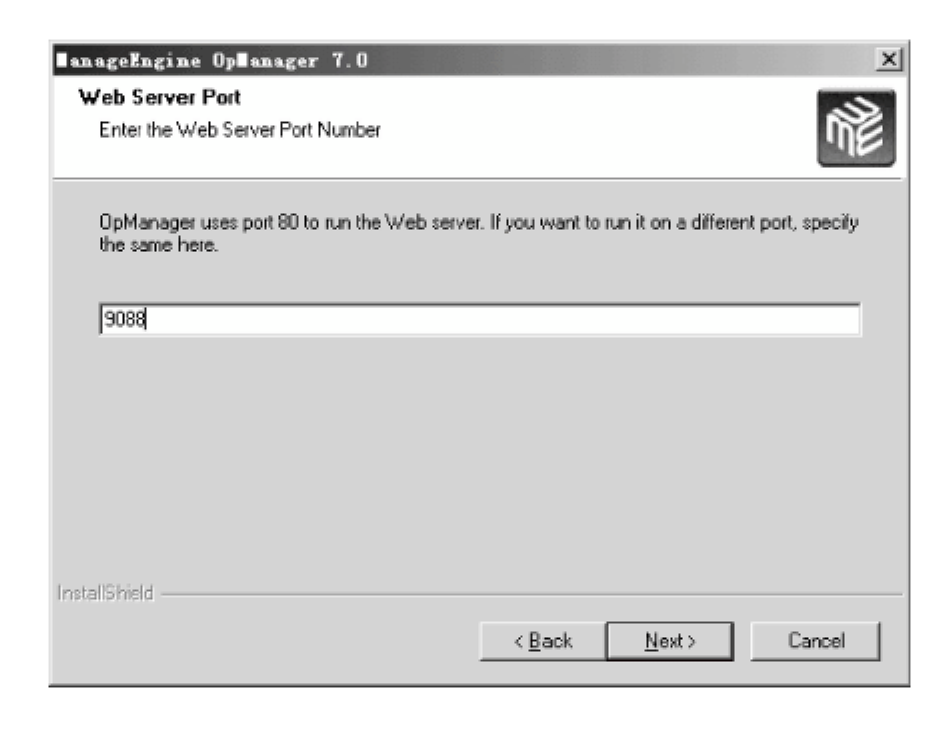


图 5-37　Web Server Port 对话框

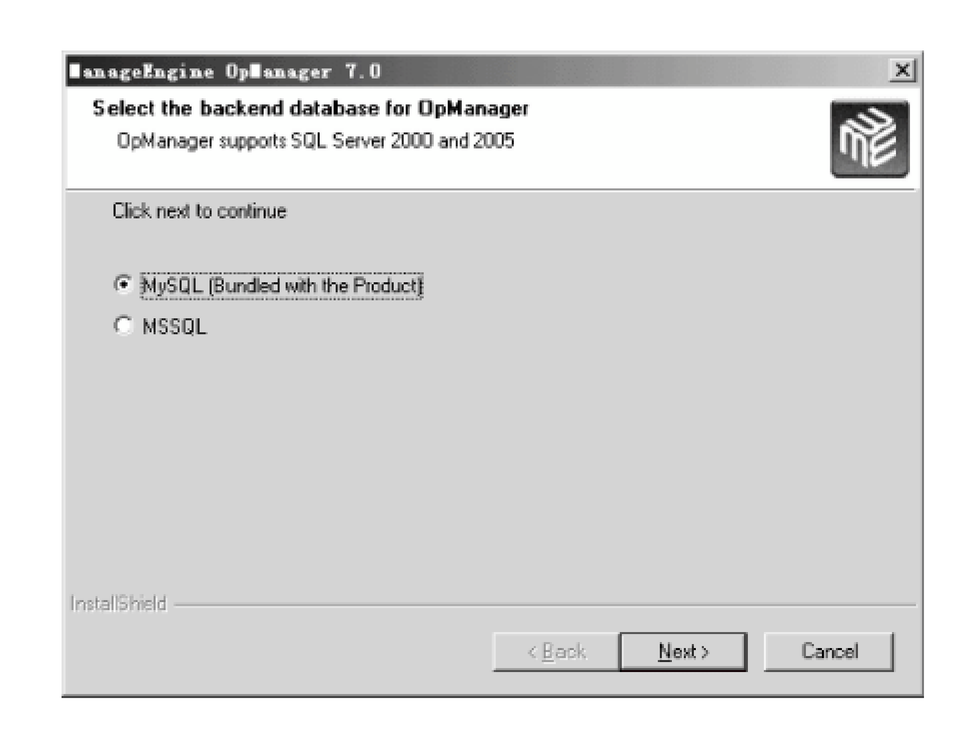


图 5-38　Select the backend database for OpManager 对话框

3. 使用发现向导发现网络设备

OpManager 安装完成后，即可从网络中的任意可以访问到该服务器的计算机上登录 OpManager，该操作更加便于管理员进行管理，这里客户端计算机使用的是 Windows Vista 系统。

(1) 在 IE 浏览器的地址栏中，输入 http://OpManager 服务器 IP 地址:9088，这里的 9088 即为在 OpManager 安装时所设置使用的端口号，例如这里输入的地址为: http://192.168.100.11:9088，按 Enter 键确认，显示图 5-39 所示的登录界面。在“用户名”和“密码”文本框中输入默认的用户名和密码，即 admin。



图 5-39　登录 OpManager

（2）单击 Login 按钮，即可登录 OpManager。第一次登录 OpManager，会自动启用发现向导，如图 5-40 所示。



图 5-40　发现向导

（3）单击 Next 按钮，显示图 5-41 所示的“凭证库”页面，并自动显示“添加凭证”对话框。在“凭证类型”下拉列表框中，选择所使用的 SNMP 版本，这里选择 SNMP v1/v2 选项。在“名称”和“描述”文本框中，分别输入凭证名称和描述信息。在“SNMP 读团体字串”和“SNMP 写团体字串”文本框中，分别输入网络所设置的读团体字符串和写团体字符串。在“SNMP 端口”文本框中，保持默认设置即可。设置完成后，单击“添加”按钮即可。



图 5-41　“凭证库”页面

（4）单击 Next 按钮，显示图 5-42 所示的“选择服务”页面。在左侧“支持的服务”列表中，选择所要添加的服务，单击 >> 按钮，添加到“所选的服务”列表中。

（5）单击 Next 按钮，显示图 5-43 所示的“发现设备”页面。选中“使用 IP 范围”单选按

钮，分别在“起始 IP”和“结束 IP”文本框中输入所要发现的 IP 地址范围。在“网络掩码”下拉列表框中，选择所要使用的网络掩码。在“要用的凭证”列表中，选中所要使用的凭证对应的复选框。



图 5-42　“选择服务”页面



图 5-43　“发现设备”页面

（6）单击 Next 按钮，即可开始“发现设备”。发现完成后，显示图 5-44 所示的“导入设备”页面，显示所有发现的设备。

（7）单击 Next 按钮，将已发现的设备添加到 OpManager 服务器中，设置添加完成后，显示图 5-45 所示的页面。

（8）单击 Finish 按钮，完成设备添加，并登录 OpManager 主页，如图 5-46 所示。

4. 用户管理

默认情况下，OpManager 会创建一个管理用户，其用户名和密码均为 admin，为了安全



图 5-44 “导入设备”页面



图 5-45 成功添加设备



图 5-46 OpManager 主页

起见，必须修改该用户的密码。如果网络中存在多个管理员，可以分别为管理员创建管理用户，并设置其相应的管理权限。

(1) 创建新用户

如果想要创建新用户，必须使用具有完全控制权限的用户，并且只能从 Web 客户端创建和管理用户。这里因为第一次登录 OpManager，使用的是系统默认的用户 admin，即具有完全控制权限的用户。

① 在 OpManager 主页中，单击"管理"按钮，如图 5-47 所示。

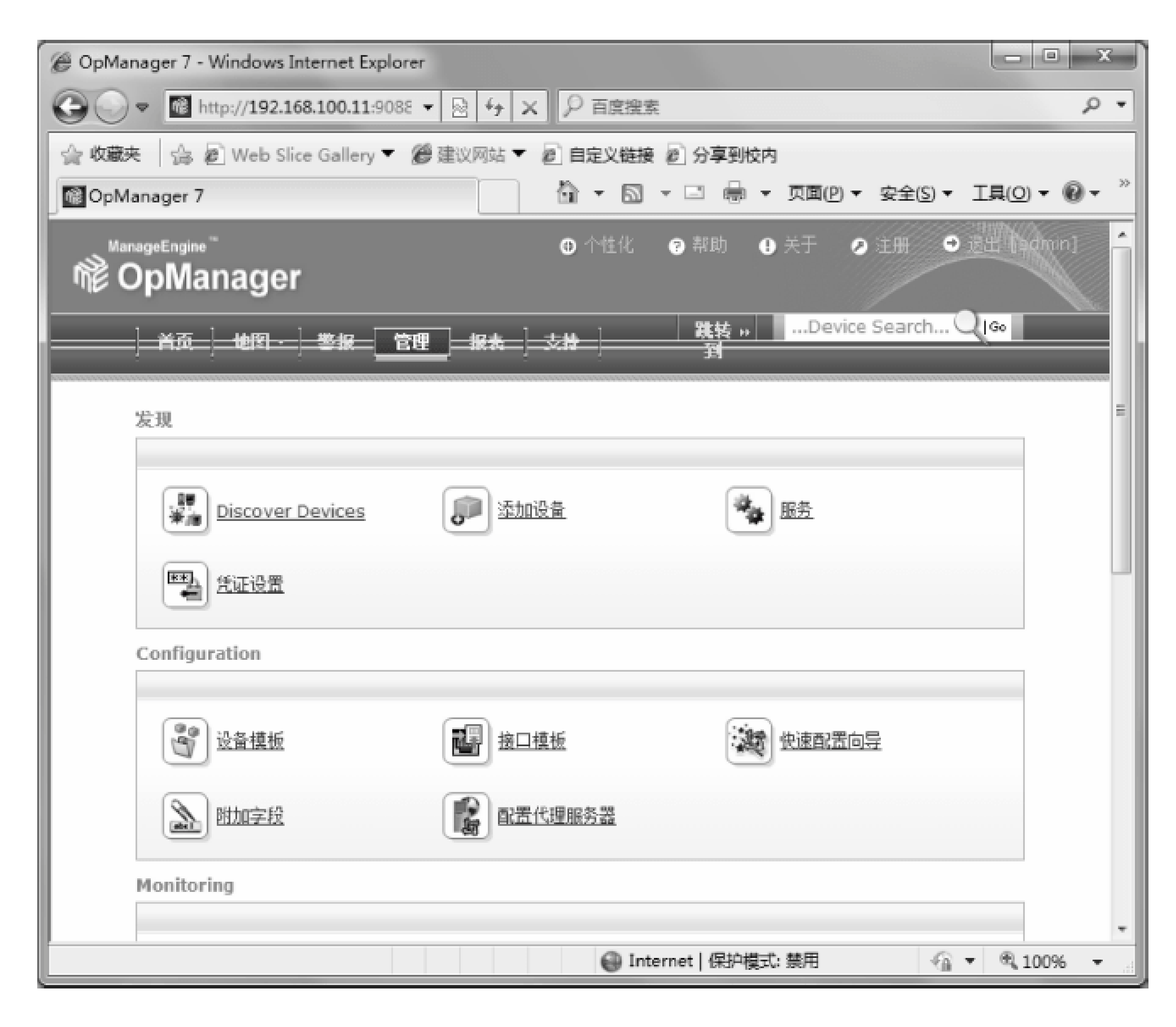


图 5-47 管理页面

② 在"工具"选项区域中，单击"用户管理器"链接，显示图 5-48 所示的"用户配置"窗口。在该窗口中，显示当前系统中存在的用户。

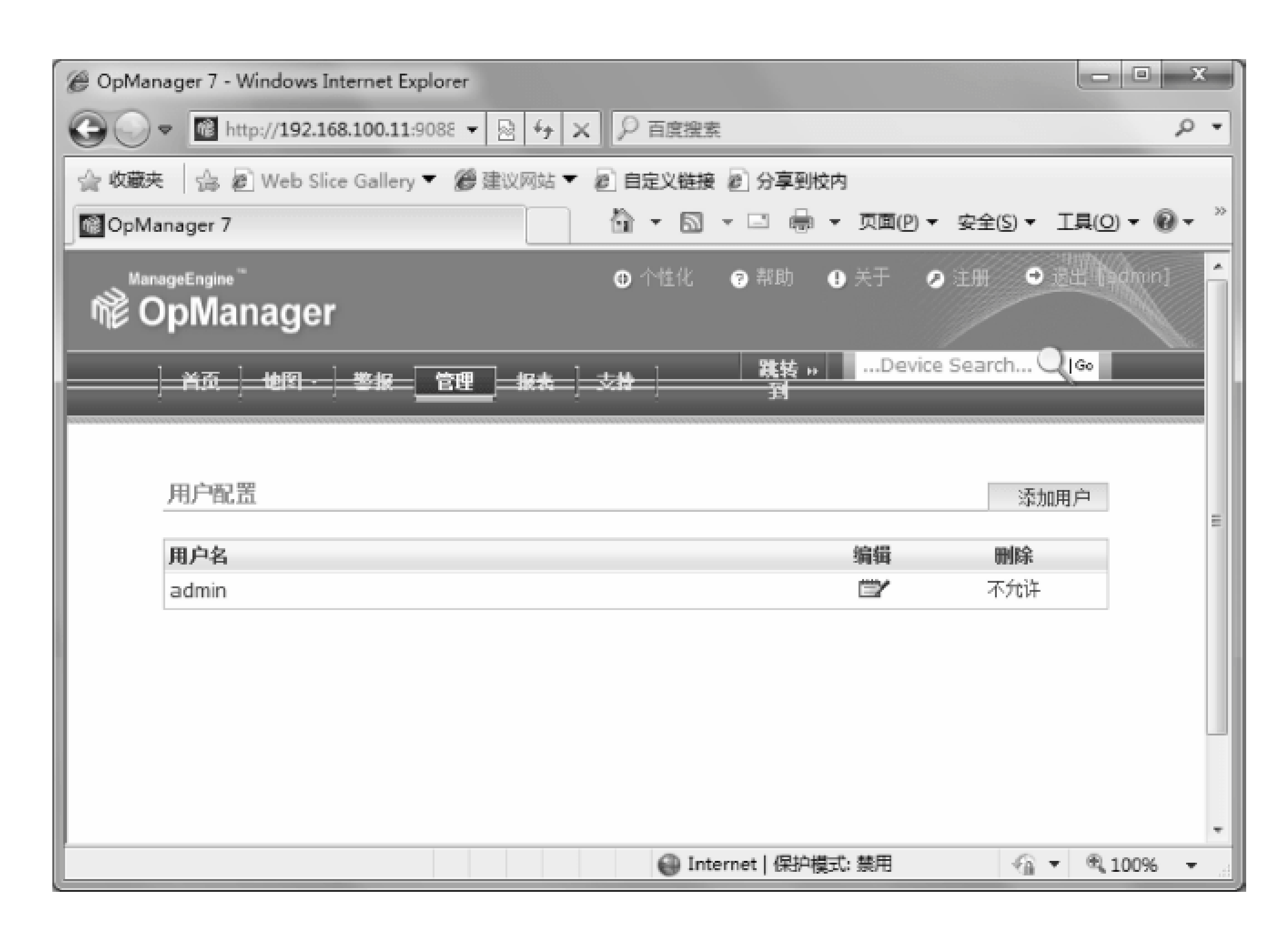


图 5-48 "用户配置"窗口

③ 单击“添加用户”按钮，显示图 5-49 所示的“添加用户”窗口。根据实际需要输入用户的详细信息，具体包括“用户名”、“密码”、“电子邮件”、“电话”等信息。在“访问明细”选项区域中，根据需要设置所添加用户的权限。

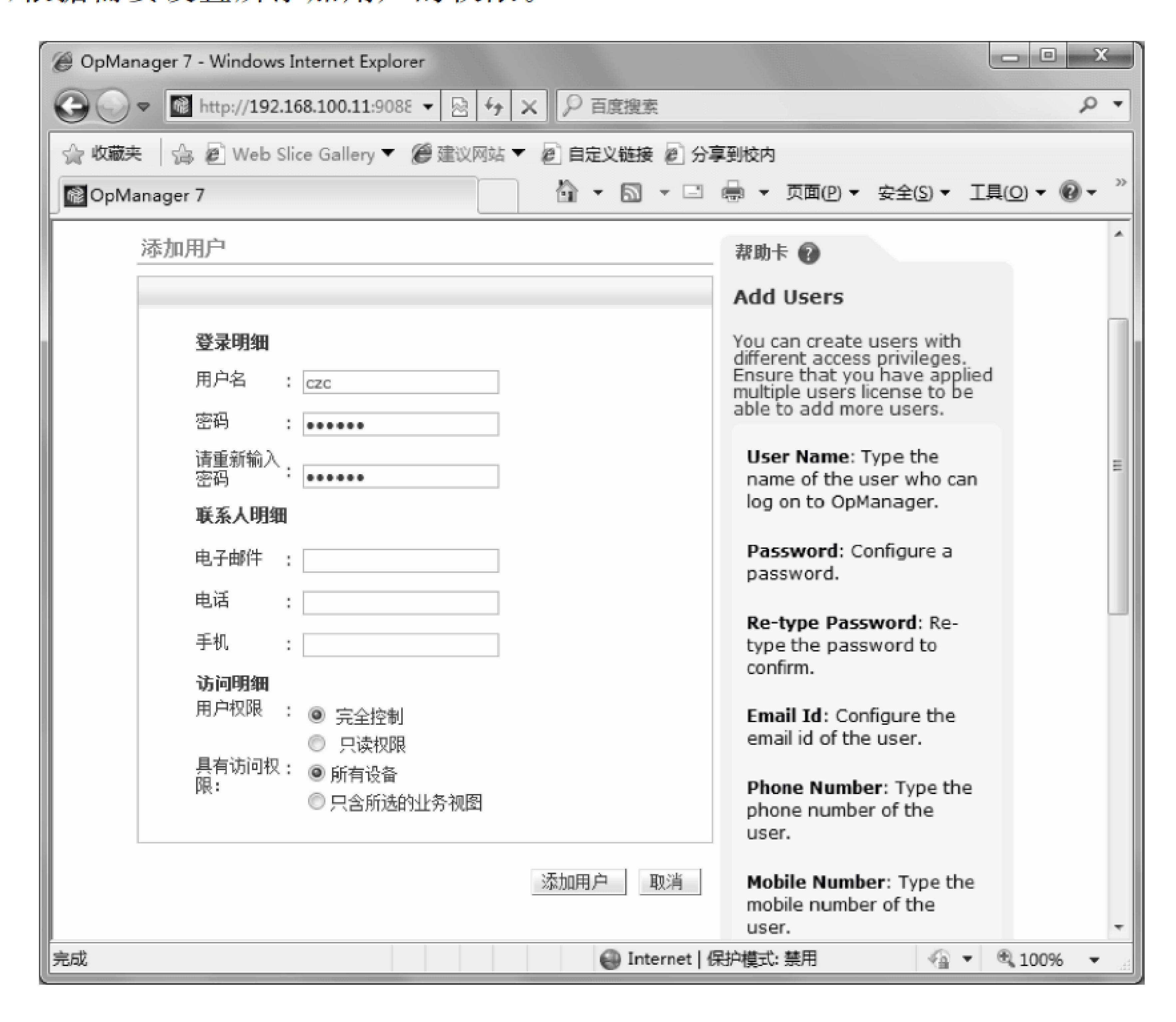


图 5-49 “添加用户”窗口

在 OpManager 中具有“完全控制”的用户的具体权限为：发现网络和设备，管理和取消管理设备，创建自定义视图，创建监视器，修改数据库维护、警报逐步升级和用户权限等，创建设备类型，配置 SNMP 陷阱处理器，配置设备的监视间隔，创建事件日志规则，配置 URL 监视器，修改设备设定，修改发现设定。

在 OpManager 中具有“只读权限”的用户的具体权限为：查看被管设备的状态、快照、图表和报表，查看、注释、确认以及清除警报，查看被管设备中已安装的软件以及活动进程列表，查看和修改资产明细。

④ 单击“添加用户”按钮，完成用户添加的设置，如图 5-50 所示。

(2) 修改用户密码

① 在“用户配置”窗口中，单击需要修改密码的用户右侧的 按钮，显示图 5-51 所示的“编辑配置文件-czc”页面。根据实际需要，修改用户的密码即可。

② 单击“确定”按钮，保存设置即可。

(3) 删除用户

① 在“用户配置”窗口中，单击需要删除的用户右侧的 按钮，显示图 5-52 所示的“真的要删除所选用户吗”提示框。

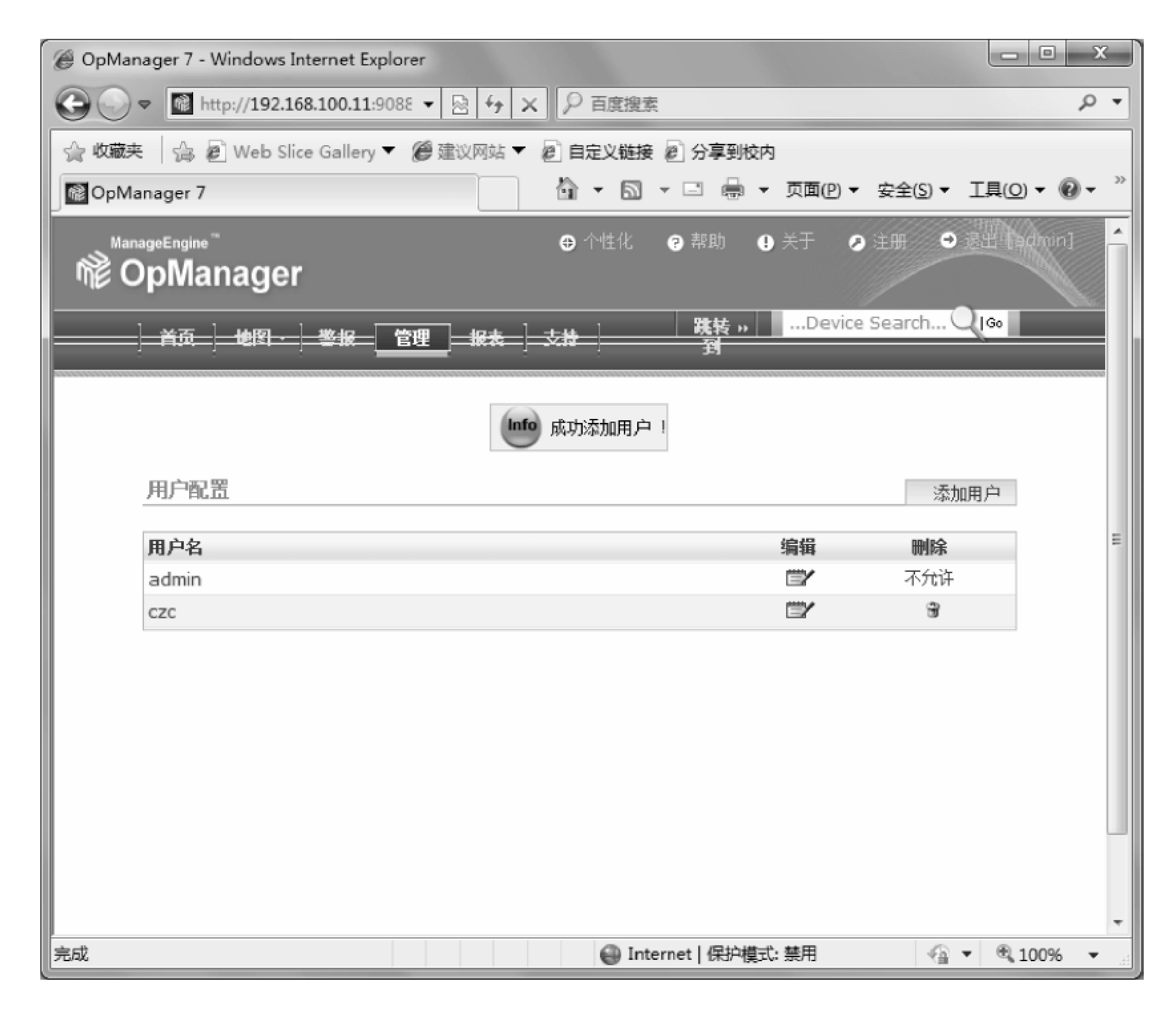


图 5-50　用户添加成功

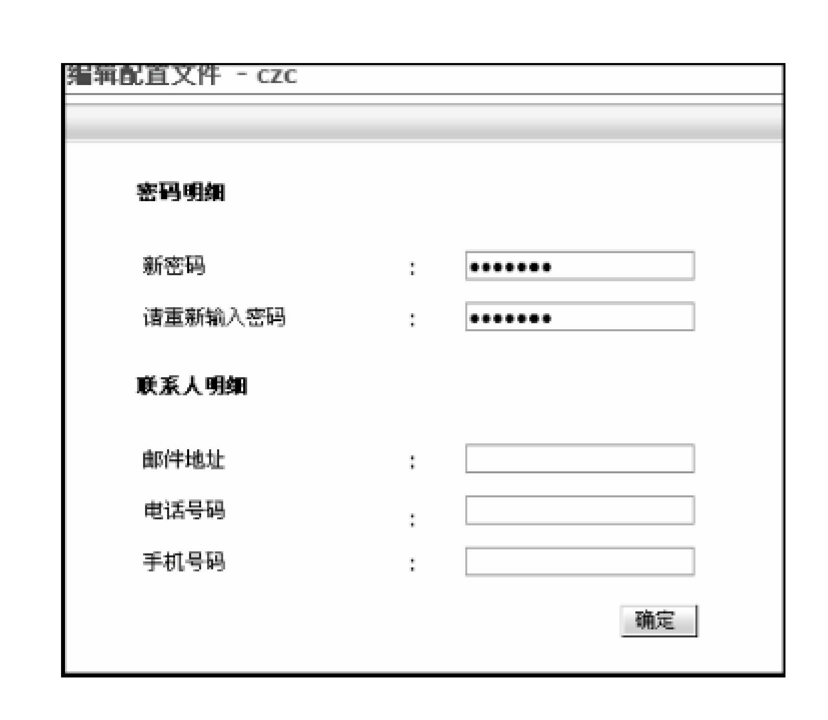



图 5-51　“编辑配置文件-czc”页面



图 5-52　“真的要删除所选用户吗”提示框

② 单击“确定”按钮，即可删除所选用户。

5. 网络发现

OpManager 使用 SNMP 和 ICMP 设定自动发现“发现向导”中所选择的网络，以及其中的所有设备。OpManager 使用 Telnet 协议来识别非 SNMP 设备的操作系统。除了发现所选网络上的设备外，OpManager 还可以扫描已发现设备上的服务。

(1) 配置 SNMP 发现

OpManager 使用 SNMP 字符串发现设备，因此，需要在网络设备上安装并启用 SNMP，当 OpManager 发现设备时，会收集许多非常有用的信息，例如活动进程、已安装软件、通信量和带宽利用率、资产明细等。配置 SNMP 发现的具体操作步骤如下。

① 在管理窗口中的“发现”选项区域中，单击“凭证设置”按钮，打开图 5-53 所示的“凭证库”页面，显示当前已经设置的 SNMP 字符串。

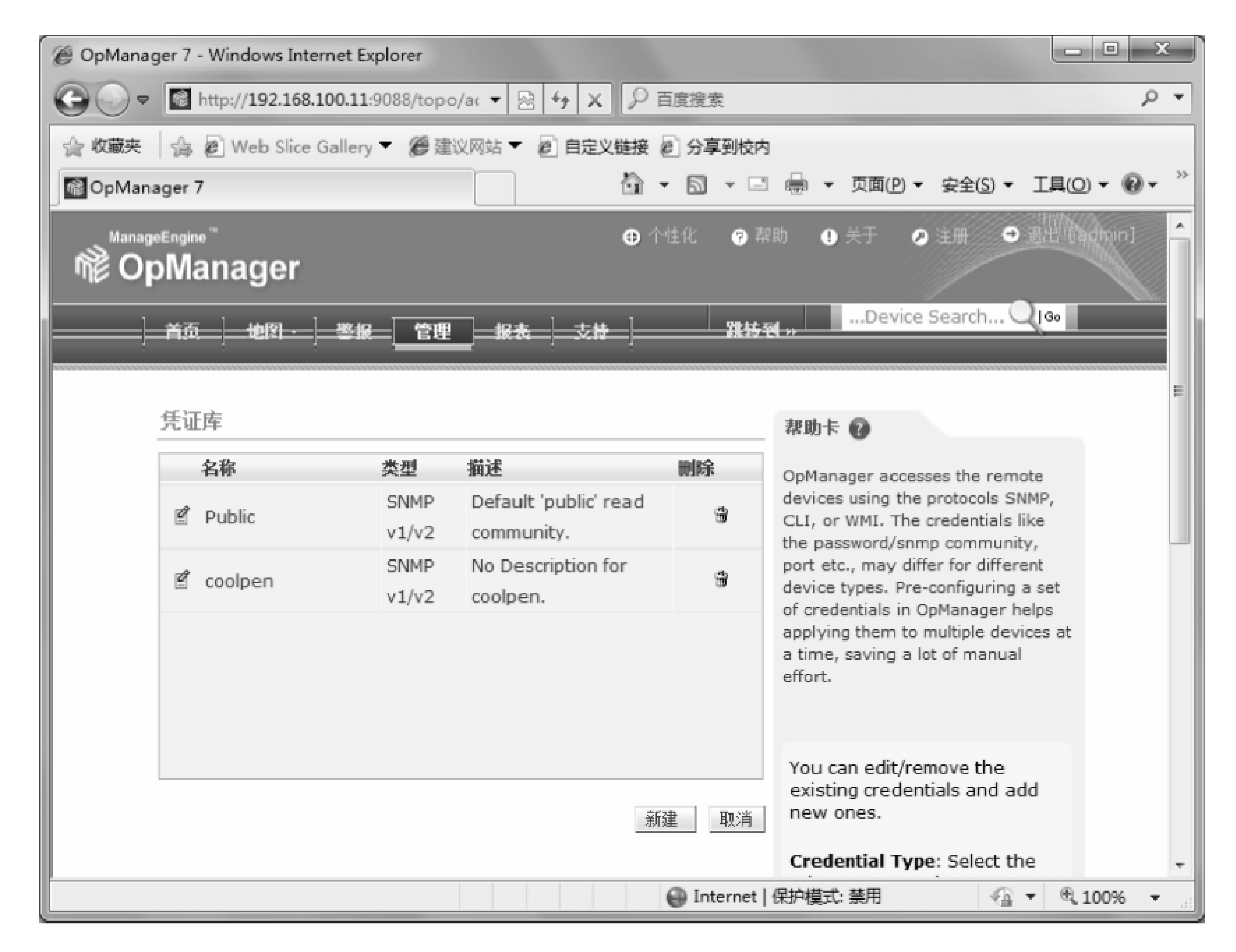


图 5-53 “凭证库”页面

② 单击“新建”按钮，显示图 5-54 所示的“添加凭证”对话框。具体设置方法可参见前面所介绍的内容，这里就不再赘述。

③ 单击“添加”按钮，即可将该凭证添加到“凭证库”中。

在“凭证库”中，单击想要编辑的凭证前的按钮，可以编辑已添加的凭证。



图 5-54 “添加凭证”对话框

(2) 发现多个网络

默认情况下，OpManager 只对已在发现向导中选择的网络执行发现，但通常情况下，网络中的设备会处于同一网络中，此时可以通过配置来发现附加网络或子网，以扩展管理范围。

① 在管理窗口中的“发现”选项区域中，单击“添加设备”按钮，打开图 5-55 所示的“发现设备”页面。选中“使用 IP 范围”单选按钮，并分别在“起始 IP”和“结束 IP”文本框中输入想要发现的网络范围，在“网络掩码”下拉列表框中选择所使用的子网掩码。在“要用的凭证”列表框中选中所使用的 SNMP 凭证对应的复选框。

② 单击“发现”按钮，开始网络设备的发现。发现完成后，显示图 5-56 所示的“导入设备”页面，在列表中显示了所有已发现的设备。需要注意的是，某些设备可能无法识别其类型，此时该设备将会显示在 Unknown 列表中。





图 5-55 “发现设备”页面



图 5-56 “导入设备”页面

③ 单击“导入设备”按钮，即可将所发现的设备导入到设备列表中。导入完成后，显示图 5-57 所示的页面。

④ 单击“发现更多设备”按钮，可以继续发现其他网络设备。单击“完成”按钮，即可完成发现设备。

（3）发现指定设备

在发现过程中，由于种种原因某些设备可能无法发现，例如当执行发现网络操作时，某些设备正处于关机状态，此时，则不能发现该设备。为了能够正常监视和管理该设备，可以使用发现指定设备的方法，手动发现该设备。

① 在管理窗口中的“发现”选项区域中，单击“添加设备”按钮，打开图 5-58 所示的“添加设备”页面。在“设备名/IP 地址”文本框中输入设备的 IP 地址。在“网络掩码”文本框中输入该设备的子网掩码。在“使用凭证”列表中选中所要使用的凭证对应的复选框。



图 5-57 导入设置完成



图 5-58 “添加设备”页面

② 单击“添加设备”按钮，即可发现设备并添加到基础架构图中。

（4）管理和取消管理设备

默认情况下，OpManager 管理所有被发现的设备，但是有一些已知的设备正处于维护之中，因此不能响应 OpManager 发出的状态轮询。可以将这些设备设置为非管理状态以避免不必要的轮询。当维护结束时，再恢复为管理状态。

① 在 OpManager 管理页面中，将鼠标移动到“地图”图标上，会自动显示图 5-59 所示的页面。



图 5-59　设备分类汇总信息

② 在页面中，单击所要取消管理的设备分类，例如这里单击 Desktops 链接，显示图 5-60 所示的设备清单列表。



图 5-60　设备清单

③ 单击想要取消管理的设备图标，显示图 5-61 所示的“快照-Ad-1”页面。在“动作”下拉菜单中，选择“取消管理”命令即可取消管理所选设备。当设备恢复后，再次选择“动作”下拉菜单中的“管理”命令即可。

6. 在特定组中导入设备

在某些情况下，软件可能无法正确识别出设备类型，例如将服务器识别为普通工作站计算机。为了能够分类监视网络设备，通常情况下，需要手动检查所有已发现并导入到软件中的设备是否已正确识别其类型。这里以在服务器组中导入设备为例进行介绍。



图 5-61 “快照-Ad-1”页面

(1) 将鼠标移动到“地图”按钮上,显示图 5-62 所示的窗口。



图 5-62 “地图”窗口

(2) 单击 Servers 链接,显示图 5-63 所示的 Servers 窗口。在“服务器”列表中,显示了当前组中所有的设备。

(3) 单击“导入”按钮,显示图 5-64 所示的“导入”对话框。在“可用的设备”列表中,选中所要导入该组中的设备名称,借助 Ctrl 键和 Shift 键,可以选择多个设备。单击 >> 按钮,将其添加到右侧“选择的设备”列表中。

(4) 单击“立即导入”按钮,即可将所选设备添加到 Servers 组中。

7. OpManager 监视 Windows 服务

OpManager 不仅可以监视网络设备,还可以监视 Windows 系统服务,例如 DHCP 服务、DNS 服务、磁盘管理、事件日志、FTP 服务、IAS 服务、IIS 服务、MySQL 等。需要注意的是,如果想要监视 Windows 服务,OpManager 必须安装在 Windows 计算机上。

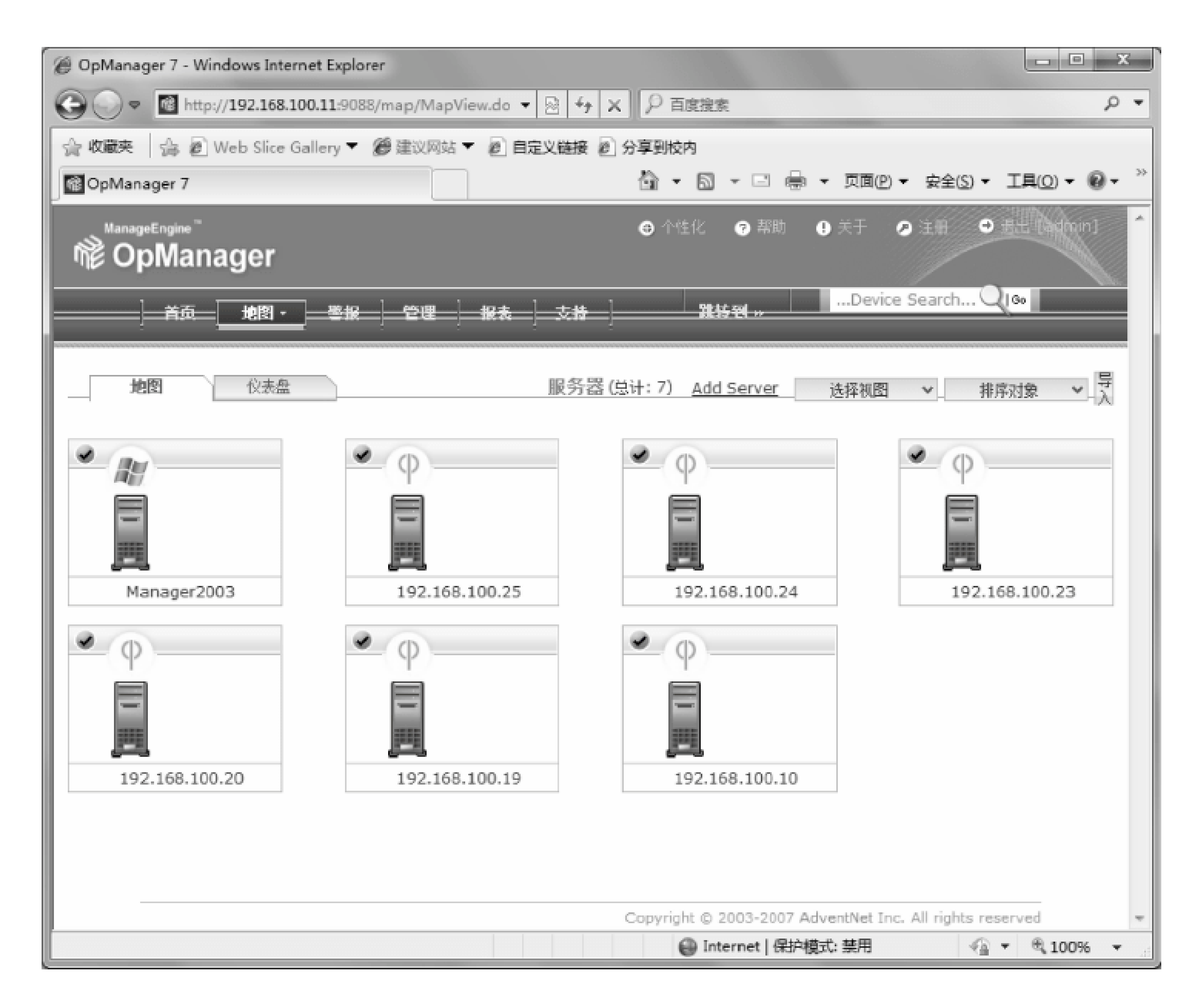


图 5-63 Servers 窗口



图 5-64 “导入”对话框

(1) 创建 Windows 服务监视器

除了 OpManager 集成的 Windows 服务监视器外，还可以根据需要创建自己特有的监视器。具体操作步骤如下。

① 在 OpManager 首页中，单击“管理”按钮。在“监视器”选项区域中，单击“Windows 服务监视器”按钮，显示图 5-65 所示的现有的服务监视器列表。

② 单击“动作”按钮，在下拉菜单中选择“新添服务”命令，显示图 5-66 所示的“添加 Windows 服务监视器”页面。在“设备名”文本框中，输入 Windows 服务器的名称。在“用户名”和“密码”文本框中，分别输入该服务器的管理员用户名和密码。

③ 单击“下一步”按钮，显示图 5-67 所示的“选择服务”页面。在“选择服务”列表中，选择所要添加的服务，借助 Shift 键和 Ctrl 键，可以同时选择多个服务。在“当服务不可用时



图 5-65　现有的服务器监视器列表

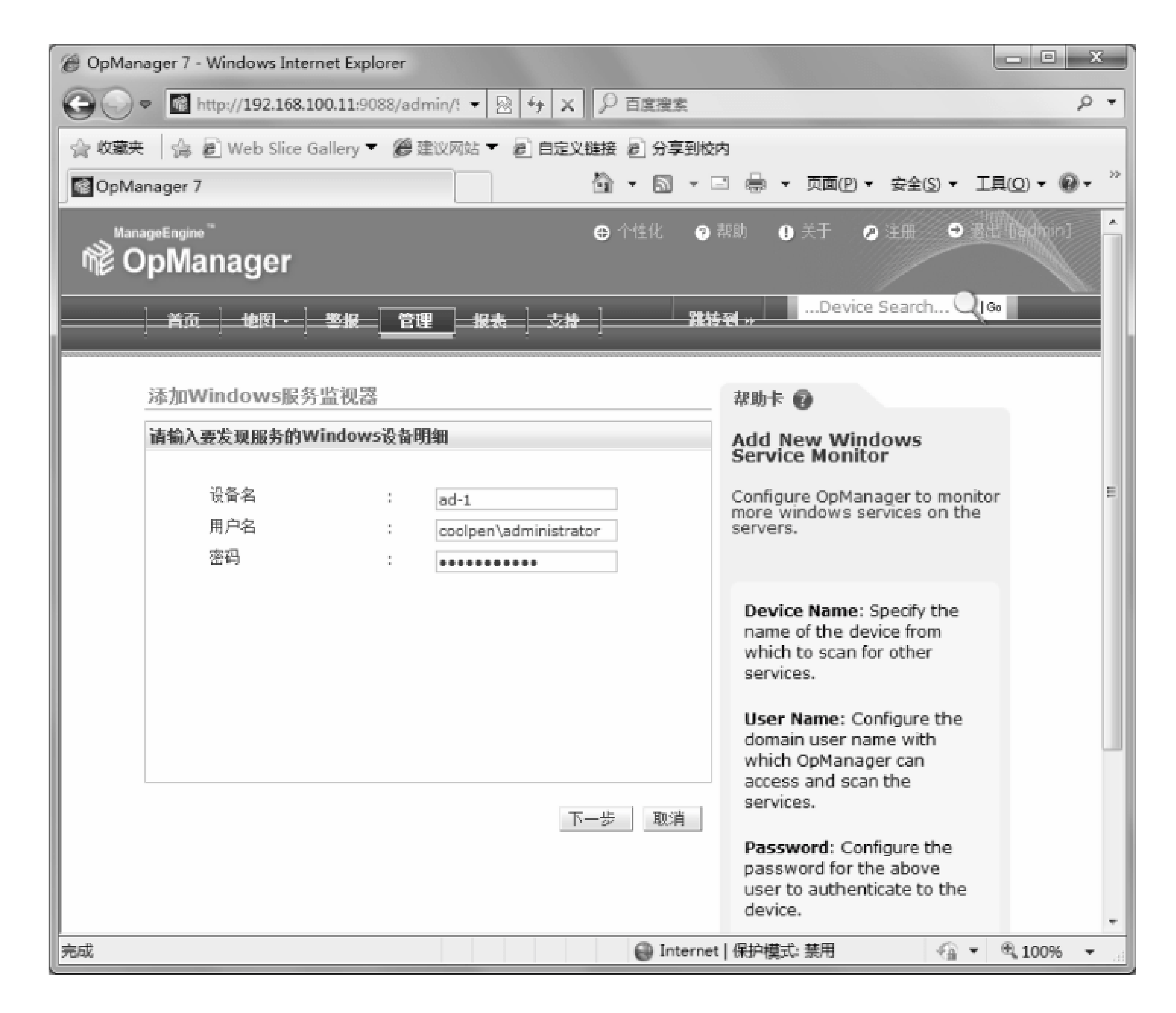


图 5-66　“添加 Windows 服务监视器”页面

执行以下动作”选项区域中，选择远程服务不可用时的操作，包括“重启服务”、“重启服务器”和“无动作”3 个单选按钮。

④ 单击“完成”按钮，完成新的 Windows 服务监视器的创建。

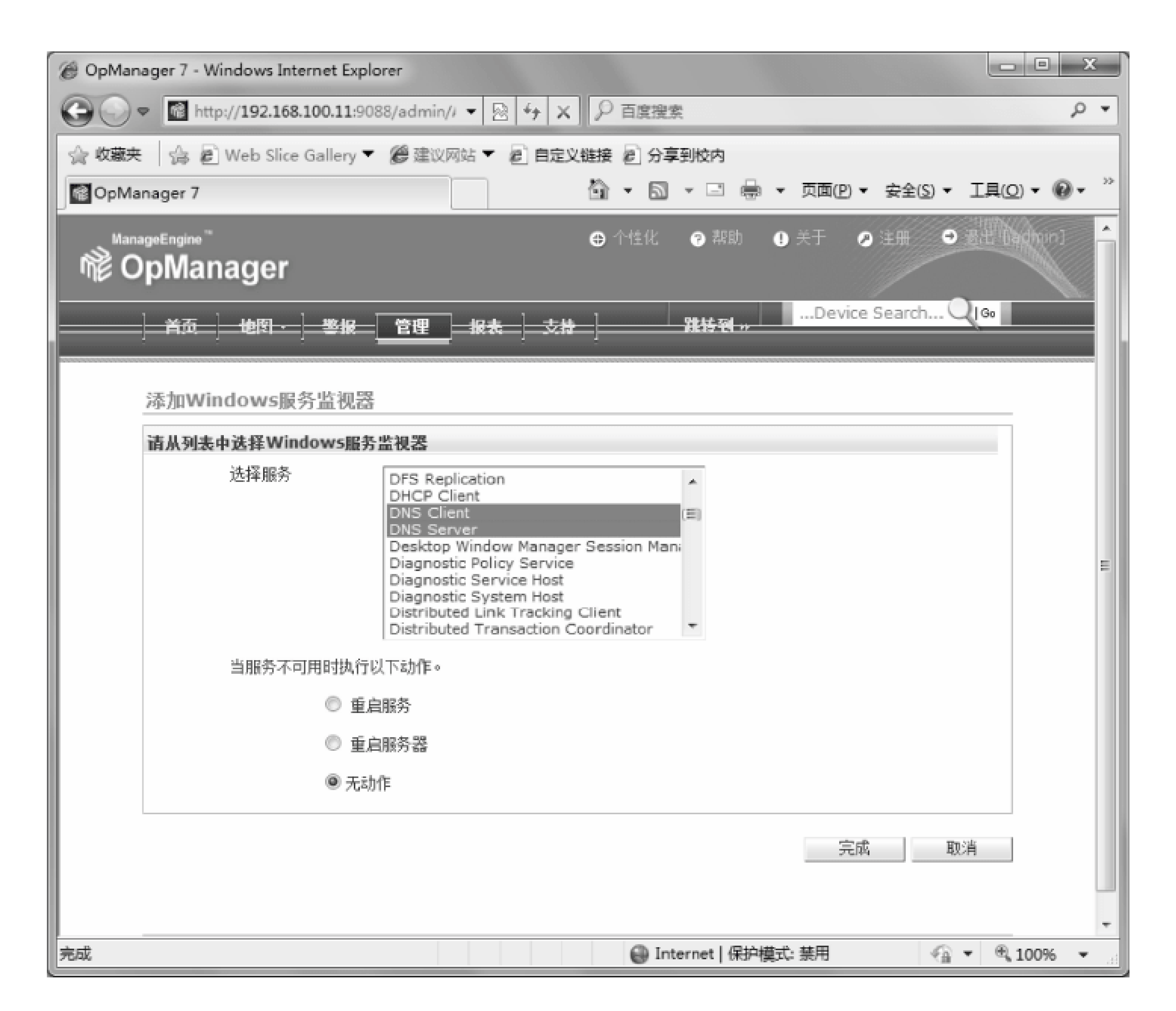


图 5-67 “选择服务”页面

(2) 将 Windows 服务监视器应用到服务器

因为 OpManager 使用 WMI 监视 Windows 服务，所以需要提供具有管理权限的用户信息。

① 在 OpManager 管理页面中，单击“管理”按钮，在“配置”选项区域中，单击“快速配置向导”按钮，显示图 5-68 所示的“快速配置向导”页面。在“要完成的任务”选项区域中，选中“为多个设备新添监视器(例如：传输监视器、服务监视器等)”单选按钮。



图 5-68 “快速配置向导”页面

② 单击“下一步”按钮，显示图 5-69 所示的“添加监视器”页面。根据需要进行选择，这里选中“选择要监控的 Windows 服务”单选按钮。

③ 单击“下一步”按钮，显示图 5-70 所示的“关联设备”页面。根据需要选择所要添加的服务名，例如这里选中 RPC 单选按钮。

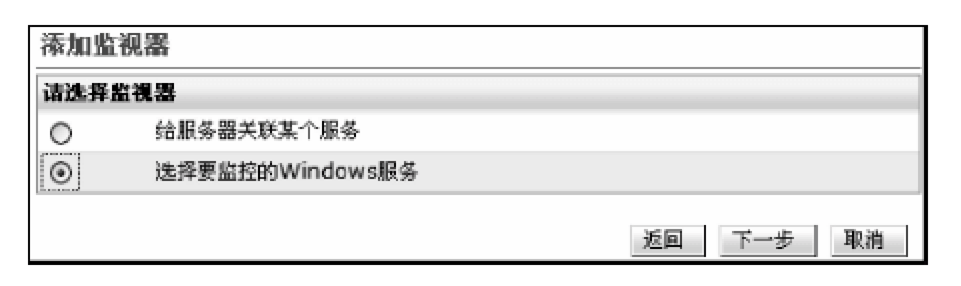


图 5-69　“添加监视器”页面



图 5-70　“关联设备”页面

④ 单击“下一步”按钮，显示图 5-71 所示的“选择服务”页面。在左侧“没有监视该服务的设备”列表中，选择所要关联的服务器名称，借助于 Ctrl 键和 Shift 键，可以选择多个设备。然后，单击 >> 按钮，将服务器添加到右侧“监视该服务的设备”列表中。



图 5-71　“选择服务”页面

⑤ 单击“完成”按钮，确认添加，成功关联后显示图 5-72 所示的“结果”页面。



关联设备

结果

设备名	结果
Files-1	RPC successfully added
Files2	RPC successfully added
Manager2003	RPC successfully added
192.168.100.8	RPC successfully added
Ad-1	RPC successfully added

返回快速配置向导

图 5-72　“结果”页面

（3）查看 Windows 服务监视内容

① 在 Servers 窗口中，单击想要查看的服务器名称，例如这里单击 AD-1，显示图 5-73 所示的“快照-Ad-1”页面。显示服务器监视信息的统计信息，例如 CPU 使用率、内

存使用率和磁盘使用率等。在“监视器”选项卡中，显示了当前服务监视信息，其中，如果在某项服务的“状态”列中，显示图标，说明该服务最近发出了警报信息。



图 5-73 “快照-Ad-1”页面

② 在“最近的警报”选项区域中，单击警报的名称，显示图 5-74 所示的“警报明细”页面。显示该服务警报的详细信息，包括重要度、状态、消息内容等。

警报明细　　确认　清除　删除　添加注释

来源	Ad-1
重要度	Service Down
最后	Mar 24,2009 05:42:18 PM
消息	Windows NT Service Telnet is Down

事件历史

状态	日期 / 时间	消息
Service Down	Mar 24,2009 05:42:18 PM	Windows NT Service Telnet is Down
Service Down	Mar 22,2009 03:26:00 AM	FTP Service is Down
Clear	Mar 22,2009 03:25:57 AM	设备正常并有应答
Attention	Mar 22,2009 03:21:08 AM	设备没有响应：可能设备关闭了或者设备太忙
Service Down	Mar 22,2009 03:15:58 AM	FTP Service is Down
Clear	Mar 22,2009 03:15:58 AM	Web Service is Up
Service Down	Mar 22,2009 03:11:04 AM	Web, FTP Services are Down
Service Down	Mar 19,2009 09:12:10 PM	FTP Service is Down
Clear	Mar 13,2009 03:24:08 PM	设备正常并有应答
Attention	Mar 13,2009 03:19:52 PM	设备没有响应：可能设备关闭了或者设备太忙

图 5-74 “警报明细”页面

③ 单击“确认”按钮，可以确认该警报信息。单击“清除”按钮，可以清除该警报信息。单击“删除”按钮，可以删除该警报信息。

(4) 查询设备中安装的软件

OpManager 可以查询某个设备上已安装软件的相关信息，设备上安装的应用越多，其性能就越低。因此，通过 OpManager 的查询软件功能，检验在某个重要的服务器或被管节

点上安装了不必要的应用。

在设备的快照页面中，单击“设备信息”按钮，在下拉列表框中选择“已安装的软件”选项，显示图 5-75 所示的“已安装的软件”窗口，显示当前设备上所安装的软件。



图 5-75 “已安装的软件”窗口

5.5 服务器群集

Windows Server 2008 故障转移群集引入了新的网络连接功能，与旧群集中的执行方法相比，这些功能有了很大转变，例如，Windows Server 2008 故障转移群集引入了对多子网的支持。

5.5.1 群集规划

在网络应用中，对于比较重要的服务，如果在网络中只部署一台服务器，当该服务出现故障时，会直接影响其所提供服务的应用。在企业网络中，文件服务器承担着数据保存与安全等任务，对于需要实时更新的数据而言，服务器的稳定运行是必不可少的。此时，则可以使用两台以上的服务器搭建服务器群集，实现服务的无缝运行。在本书的网络环境中，因为文件服务器处于非常重要的地位，且需要保持 24 小时在线，即需要通过配置文件服务器群集来保证文件服务器的稳定。另外，由于数据保存在多个服务器上，需要使用分布式文件系统(DFS)，在文件服务器上提供一个逻辑访问点，使网络中的用户在访问时，只需要访问文件服务器中的单一访问点，而不需要在多台服务器间分别访问。

部署文件服务器群集的两台服务器必须具有两块网卡：一块用于连接专用网络(IP 地址设置为网络中未使用的网络地址段即可，这里设置 IP 地址网络为 192.168.150.0/24)；另一块用于连接企业网络(IP 地址设置为企业网地址，这里设置为服务器网络段 IP 地址段，即 192.168.100.0/26)。目前，大多数的服务器都标配了两块网卡，因此，不再需要用户另备网卡。

另外，在开始部署群集前，需要首先将外部存储设备连接到服务器，并初始化存储设备。因为在文件服务器上会保存大量的数据，因此存储设备的空闲空间也是管理员必须引起注意的问题。

群集安装前，还应进行如下准备操作。

(1) 在群集节点上安装操作系统

先不连接外置的磁盘阵列，在每个节点的计算机上安装 Windows Server 2008 操作系统，分别为计算机指定名称，为两块网卡设置 IP 地址信息。

安装完成之后，关闭群集的每个节点，并将共享的磁盘阵列连接到群集的每个节点。

(2) 将群集升级到 Active Directory 服务器

用于实现群集的服务器，都必须添加至域，并作为域外控制器。

(3) 格式化群集使用的磁盘

除了由群集共享管理的 SCSI 阵列外，作为群集节点的服务器还必须单独使用一个分区用来存储群集日志。因此，应当为群集日志专门创建一个容量为 500MB 的分区，并使用 NTFS 文件系统进行格式化。

然后，将 SCSI 阵列挂接到计算机上，对阵列(在计算机上表现为一个磁盘)进行初始化操作，并格式化为 NTFS 系统。

需要注意的是，有的磁盘阵列系统，需要使用厂商提供的专用工具软件才能安装或创建群集，或者使用专用的工具软件才能对共享的磁盘阵列进行操作。

5.5.2 群集的连接

故障转移群集的基本应用拓扑如图 5-76 所示，此时应用程序服务器与数据库服务器直接连接，数据库服务器则直接与存储设备相连。当客户端计算机访问应用程序服务器时，应用程序服务器则可以从数据库服务器中读取数据。该应用的缺点是当数据库服务器发生故障时，应用程序服务器也将不能再访问这些数据。这个问题可以通过部署服务器群集来解决。客户端计算机通过群集发布的虚拟 IP 地址和主机名作为应用程序使用。

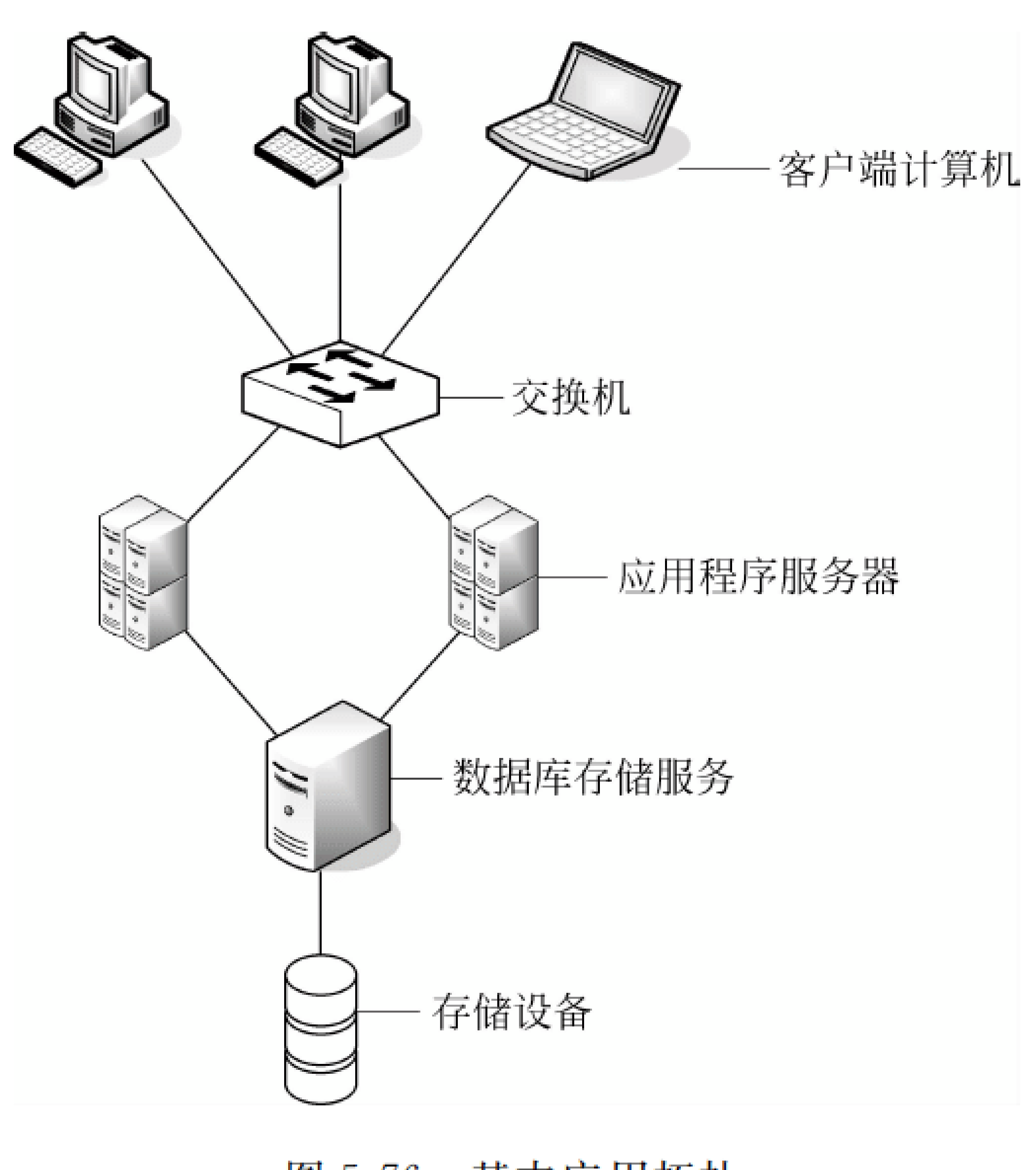


图 5-76 基本应用拓扑

5.5.3 故障转移群集的软硬件要求

实施群集服务，要求具有以下硬件。

(1) 在每个服务器的启动分区上，安装 Windows 服务器版本操作系统。需要注意的是，不能在服务器之间共享启动分区。

（2）支持SCSI或者光纤信道的独立的存储适配器，用于实现与共享存储设备的连接。该适配器必须与用于安装操作系统的硬盘控制器分开。

（3）每个服务器上都必须拥有两块PCI网卡，分别用于连接至专用网络（节点之间的连接）和企业网络（连接至企业局域网络）。

（4）一个或多个能够连接所有服务器的外部驱动器。在群集节点之间共享这些外部驱动器，一般情况下，外部驱动器是SCSI驱动器，并且采用RAID技术，以保障数据存储安全，或使用虚拟存储软件，达到类似的功能。

（5）拥有可以将各个外部驱动器与服务器连接在一起的电缆。

（6）每台服务器的内存、CPU和硬盘配置应当完全相同。如果节点的配置较低，没有支持应用程序的必要硬件，将无法在发生故障时实现故障转移，从而保证网络服务的连续、稳定。因此，群集中的每个节点，都应当满足网络服务正常运行所要求的最低配置。

（7）群集中所有服务器的全部硬件都应当完全一致，包括各种适配器（如网卡、SCSI卡、显卡等）的插槽位置、板卡品牌，以及与节点外部驱动器连接的电缆。

在为群集选择共享驱动器时，应当考虑以下要求。

（1）群集使用的所有共享驱动器（包括为仲裁资源使用的驱动器）必须物理连接到群集的所有节点上。

（2）在群集投入使用之前，必须检验并保证可以从每个节点访问共享驱动器。

（3）在使用SCSI驱动器时，每个驱动器和每个SCSI适配器必须拥有唯一的SCSI ID。

（4）每个共享磁盘必须配置为基本磁盘，而不是动态磁盘。

（5）共享磁盘上的每一个分区必须使用NTFS文件系统进行格式化。

若欲实现群集，还必须满足以下网络要求。

（1）每个节点安装两块网卡：一个连接到企业网络；另一个连接到专用网络。

（2）必须为群集选择一个唯一的NetBIOS名称。客户端使用该名称访问群集中的资源。

（3）实施双节点解决方案时，群集需要至少5个唯一的IP地址。其中，两个地址是专用IP地址，用于节点之间的通信；两个是企业网络IP地址，用于连接到局域网络。第5个地址也是企业网络IP地址，由群集自己使用。

（4）群集中的每个节点必须配置为同一个域的一部分。一个节点可以是域控制器，其他节点可以是域成员。如果决定实施域控制器，可以使其成为小域的域控制器，从而减少系统资源开销。

（5）在与节点相同的域中，必须创建域用户账户。可是，如果存在信任关系，账户可以驻留在其他域中。这个账户由运行在每个节点上的群集服务使用。

故障转移群集中的所有服务器，除安装Windows Server 2008操作系统外，还需要以下故障转移群集的网络基础结构和拥有以下域权限的管理账户。

（1）网络设置和IP地址：当针对网络使用相同的网络适配器时，需要在这些适配器上使用相同的通信设置（如速度、双工模式、流控制和媒体类型）。另外，还要比较网络适配器与所连接的交换机之间的设置，并确保设置不发生冲突。

(2) DNS：群集中的服务器必须使用域名系统(DNS)来进行名称解析。可以使用 DNS 动态更新协议。

(3) 域角色：群集中的所有服务器必须处于相同的 Active Directory 域中。另外，所有的群集服务器应具有相同的域角色(成员服务器或域控制器)，建议将所有服务器的角色升级为域成员服务器。

(4) 客户端：客户端必须能够连接到群集服务器，并且必须运行与群集服务器提供的服务兼容的软件。

(5) 用于管理群集的账户：首次创建群集或者向群集中添加服务器时，必须使用对该群集中所有服务器具有管理员权限的账户登录到域。

注意：*与 Windows Server 2003 相比，Windows Server 2008 中群集服务运行的方式发生了变化。在 Windows Server 2008 中，没有群集服务账户。群集服务将在一个提供了服务所需的特定权限的特定上下文中自动运行(与本地系统上下文相似，但权限减少)。*

5.5.4 部署存储服务

群集服务需要存储设备支持，这里使用虚拟存储设备来代替 SCSI 设备。然后在欲部署故障转移群集的成员服务器上使用"iSCSI 发起程序"连接到存储设备。

1. 节点服务器 IP 配置

群集系统包括两套网络：一套是对外提供网络服务的网络；另一套是群集成员服务器间连接的网络。

(1) 每个节点服务器上均拥有静态 IP 地址，服务器群集不支持使用由动态主机配置协议服务器分配的地址。

(2) 每个群集成员服务器至少必须拥有两个网络适配器：一个用于连接客户端的"内部网络测试"的网络；另一个用于连接群集成员服务器对数据库服务器的网络。

(3) 所有节点服务器都必须拥有两个面向公用和专用通信的物理独立的局域网或虚拟局域网。

2. 配置服务器的 iSCSI 存储服务

在群集服务中的第一台服务器添加 iSCSI 存储服务之前，需要将该服务器添加到 Active Directory 中，并以域管理员身份登录。另外，该服务器和域控制器必须启用"网络发现"功能。需要注意的是，如果服务器启用防火墙，将有可能会影响连接到存储设备。

(1) 在"控制面板"窗口中，双击"iSCSI 发起程序"图标，运行 iSCSI 发起程序。如果是第一次使用"iSCSI 发起程序"，显示图 5-77 所示的 Microsoft iSCSI 对话框，提示管理员 iSCSI 服务没有运行，必须启动该服务并在以后每次开机时自动启动 iSCSI 服务。

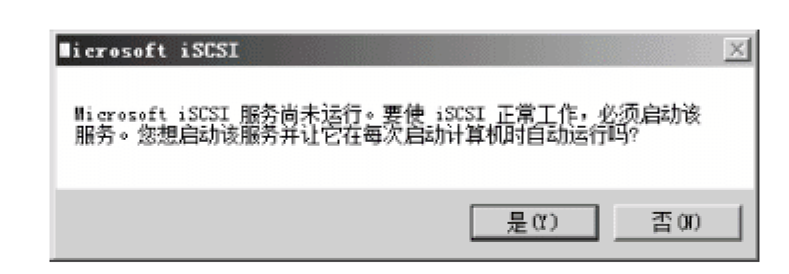


图 5-77 Microsoft iSCSI 对话框

(2) 单击"是"按钮，显示图 5-78 所示的对话框，提示需要允许 iSCSI 服务通过防火墙。

(3) 单击"是"按钮，打开"iSCSI 发起程序 属性"对话框。选择图 5-79 所示的"发现"选项卡。

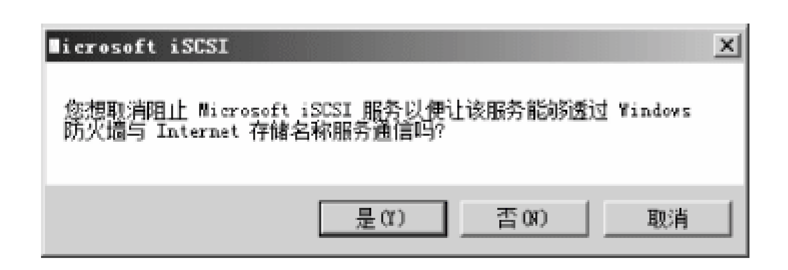


图 5-78　提示需要允许 iSCSI 服务通过防火墙



图 5-79　“发现”选项卡

(4) 单击“添加门户”按钮，显示图 5-80 所示的“添加目标门户”对话框。在“IP 地址或 DNS 名称”文本框中，输入存储服务器的 IP 地址或者 DNS 名称。

(5) 单击“确定”按钮，关闭“添加目标门户”对话框，返回“发现”选项卡，将存储服务器添加到“目标门户”列表中。选择图 5-81 所示的“目标”选项卡，在“目标”列表中，显示在域控制器中创建的虚拟磁盘。

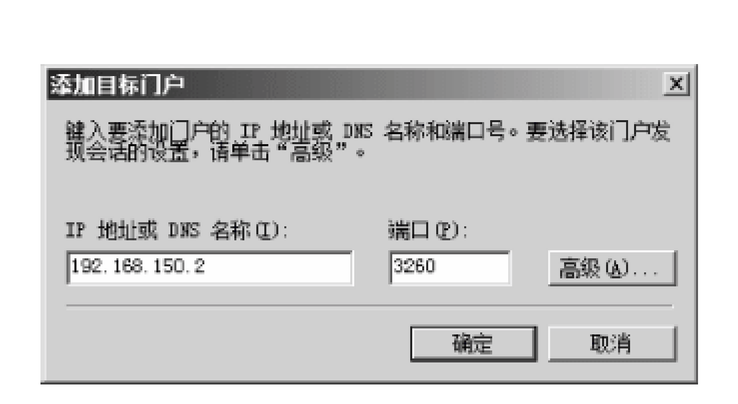


图 5-80　“添加目标门户”对话框

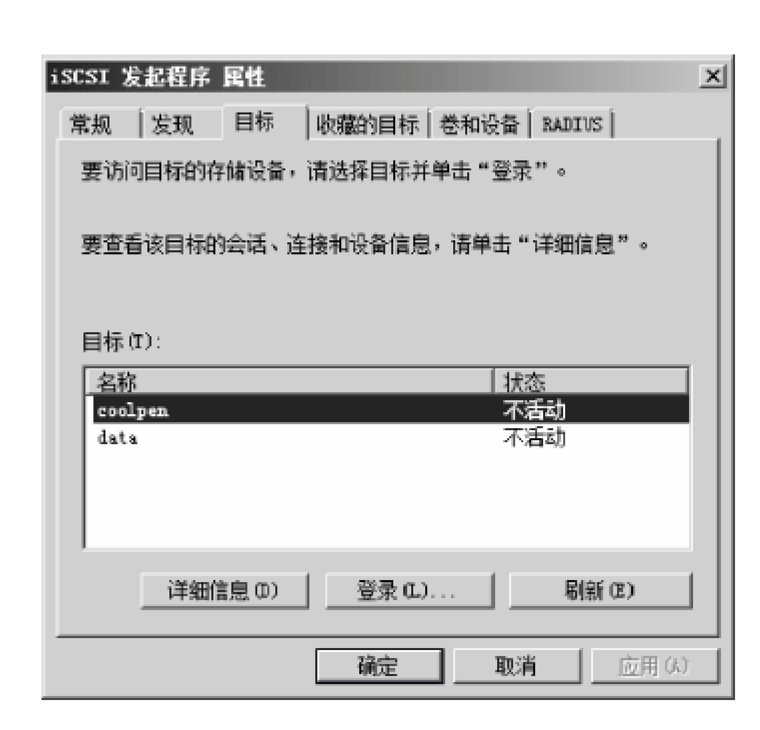


图 5-81　“目标”选项卡

(6) 选择其中任何一块磁盘，单击“登录”按钮，显示图 5-82 所示的“登录到目标”对话框。选中“计算机启动时自动还原此连接”复选框，使计算机在启动时自动连接到该磁盘。

(7) 单击“确定”按钮，关闭“登录到目标”对话框，返回到“目标”选项卡。重复操作，可连接其他磁盘，如图 5-83 所示。

(8) 单击“确定”按钮，完成 iSCSI 服务的设置。

(9) 在“服务器管理器”窗口中，依次展开“服务器管理器”→“存储”→“磁盘管理”目录，可以查看已经成功添加了的磁盘。

(10) 右击“磁盘”并在快捷菜单中选择“联机”命令，然后再右击该磁盘并从快捷菜单中选择“初始化磁盘”命令。此时，即可开始使用这些磁盘，如图 5-84 所示。

第二台服务器配置 iSCSI 的方法与第一台服务器的配置方法完全相同，具体操作这里就不再赘述。



图 5-82 “登录到目标”对话框

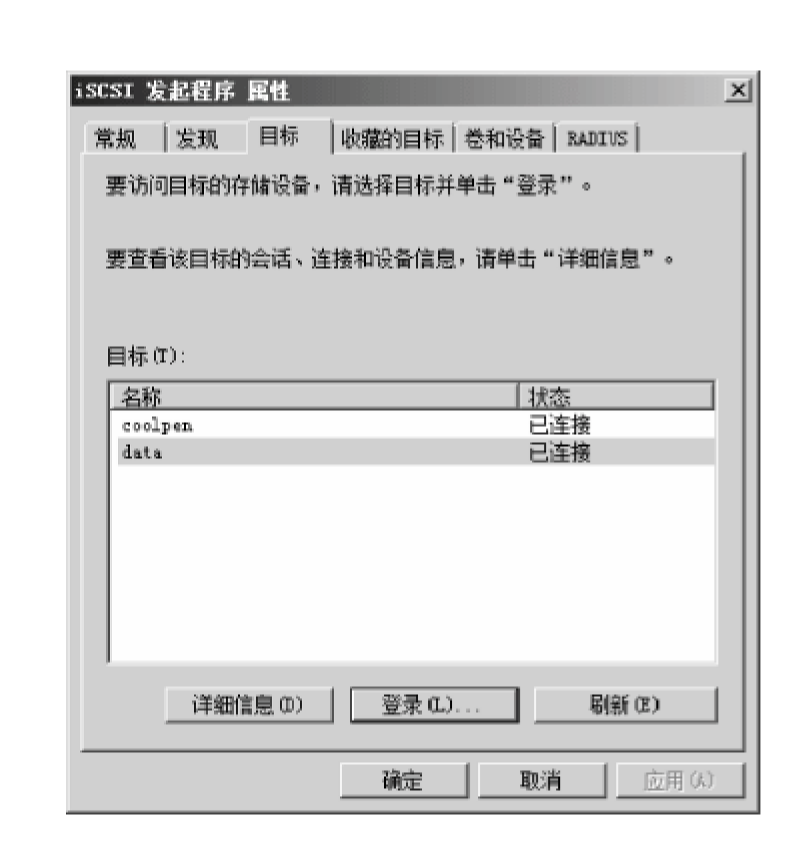


图 5-83 成功连接到磁盘



图 5-84 初始化磁盘

5.5.5 安装故障转移群集功能

故障转移群集是 Windows Server 2008 的一项单独功能，在安装 Windows Server 2008 时，故障转移群集作为可选功能，需要管理员根据需要定制安装。在群集的两台服务器安装故障转移群集的操作方法完全相同，这里仅以第一台服务器为例进行介绍。

(1) 在“服务器管理器”窗口中，依次展开“服务器管理器”→“功能”目录。在右侧窗口中，单击“添加功能”按钮，显示图 5-85 所示的“选择功能”对话框。在“功能”列表中，选中“故障转移群集”复选框。

(2) 单击“下一步”按钮，显示“确认安装选择”对话框。单击“安装”按钮，开始安装故障转移群集，安装完成，显示图 5-86 所示的“安装结果”对话框。

(3) 单击“关闭”按钮，完成故障转移群集的安装。依次选择“开始”→“管理工具”→“故障转移群集管理”命令，打开图 5-87 所示的“故障转移群集管理”窗口。



图 5-85　“选择功能”对话框



图 5-86　“安装结果”对话框

5.5.6　部署故障转移群集

与早期服务器群集相比，Windows Server 2008 提供群集部署向导，可以简单快捷地部署群集。Windows Server 2008 的群集服务对 DHCP 服务、打印服务、文件服务等基础服务提供支持。另外，在 Windows Server 2008 中，提供了完整群集部署指南，可以指导管理员顺利地完成群集部署操作。

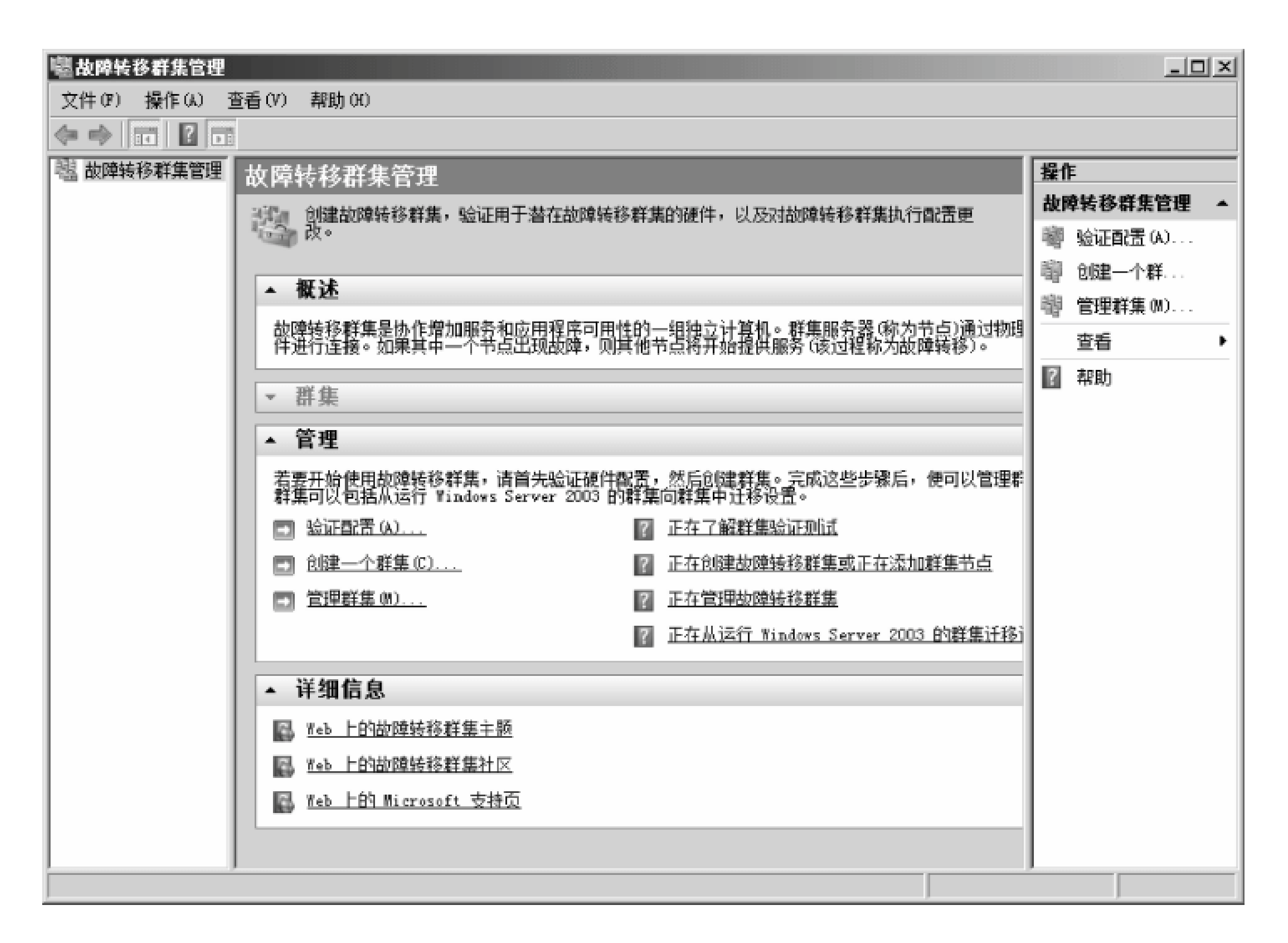


图 5-87 “故障转移群集管理”窗口

1. 验证故障转移群集

在部署故障转移群集前，首先需要使用故障转移群集服务提供的“验证配置向导”，对当前的环境进行验证，只有验证通过后才可以开始部署故障转移群集。具体操作步骤如下。

(1) 在“故障转移群集管理”窗口中，单击“验证配置”链接，启动“验证配置向导”，显示“开始之前”对话框。

(2) 单击“下一步”按钮，显示“请选择服务器或群集”对话框，设置欲部署群集的一组服务器。

(3) 单击“浏览”按钮，显示图 5-88 所示的“选择计算机”对话框。在“输入对象名称来



图 5-88 “选择计算机”对话框

选择(示例)”文本框中输入服务器的名称,单击“检查名称”按钮,检查所输入的名称是否正确。也可以单击“高级”按钮,查找服务器。

(4)单击“确定”按钮,返回“请选择服务器或群集”对话框,将选择的节点服务器添加到“选定的服务器”列表中,如图 5-89 所示。



图 5-89 “请选择服务器或群集”对话框

(5)单击“下一步”按钮,显示图 5-90 所示的“正在测试选项”对话框。用户可根据需要选择所需的测试方案,为了能够全面地测试配置内容,建议选中“运行所有测试(推荐)”单选按钮。



图 5-90 “正在测试选项”对话框

(6)单击“下一步”按钮,显示图 5-91 所示的“确认”对话框。在中间列表中,显示了所有的测试内容。

(7)单击“下一步”按钮,即可开始测试选择的节点服务器。测试完成后,显示图 5-92 所示的“摘要”对话框,可以查看所有的验证报告。

单击“查看报告”按钮,可以查看详细的群集验证报告,如图 5-93 所示。

(8)关闭 Internet Explorer 浏览器,返回到“摘要”对话框,单击“完成”按钮,关闭“摘要”对话框,完成群集的验证。



图 5-91 “确认”对话框



图 5-92 “摘要”对话框

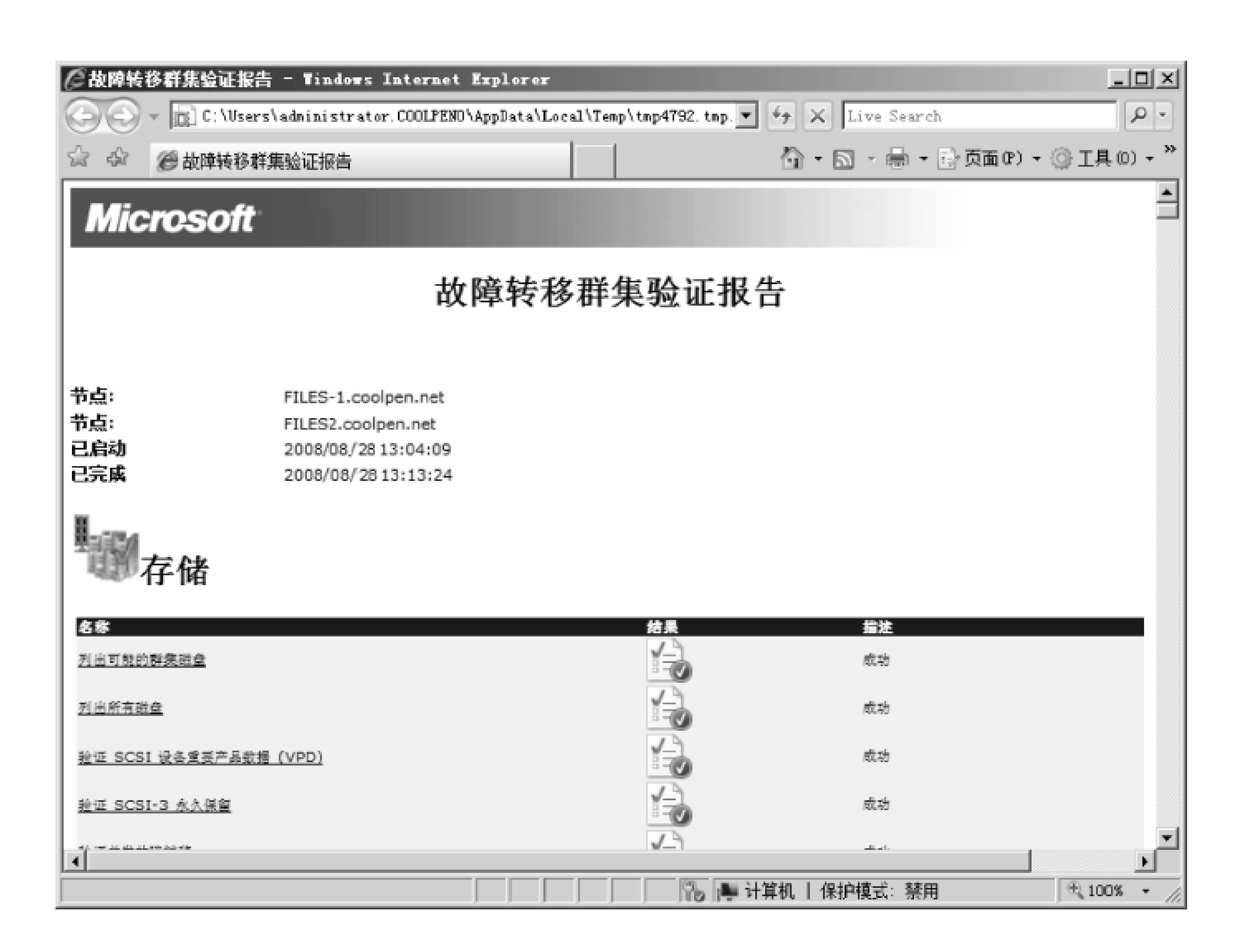


图 5-93 详细的验证报告

2. 创建故障转移群集

当所有验证均通过测试后，即可开始部署故障转移群集。创建故障转移群集可以在任意一台成员服务器上操作，当创建完成后，会自动同步到其他服务器上。具体操作步骤如下。

(1) 在“故障转移群集管理”窗口中，单击“创建一个群集”按钮，启动“创建群集向导”，显示图5-94所示的“开始之前”对话框。



图 5-94 “开始之前”对话框

(2) 单击“下一步”按钮，显示“选择服务器”对话框，添加要加入群集的所有服务器名称。具体操作方法同验证故障转移群集方法相同，这里就不再赘述，添加完成后如图5-95所示。



图 5-95 “选择服务器”对话框

(3) 单击“下一步”按钮，显示图5-96所示的“用于管理群集的访问点”对话框。在“群集名称”文本框中输入群集的名称。在“地址”文本框中输入群集使用的IP地址。

(4) 单击“下一步”按钮，显示图5-97所示的“确认”对话框。提示已准备好创建群集，并显示群集名称、节点服务器名称、群集IP地址等信息。

(5) 单击“下一步”按钮，启动群集配置进程，开始配置故障转移群集。配置完成后，显示图5-98所示的“摘要”对话框，显示已经成功创建群集。单击“查看报告”按钮，可以查看配置转移故障群集的详细过程。



图 5-96 “用于管理群集的访问点”对话框



图 5-97 “确认”对话框



图 5-98 “摘要”对话框

（6）单击“完成”按钮，完成群集的创建，创建完成的群集被添加到“故障转移群集管理”控制台窗口中，如图 5-99 所示。



图 5-99 完成创建故障转移群集

此时，即可在群集中部署所需的网络应用程序，例如 DHCP 服务、打印服务、文件服务等。

5.5.7 部署 DFS 服务器群集

借助于分布式文件系统(DFS)，可以为网络中的所有共享文件提供一个访问点和一个逻辑树结构，使分布在多个服务器上的文件如同位于网络上的一个位置一样显示在用户面前，而无论这些共享资源位于网络的什么地方。而且，还可以将一些文件同时放在多台服务器内，当用户读取文件时，DFS 会从不同的服务器为用户读取数据，减轻一台服务器的负担，且即使有一台服务器发生故障，DFS 仍然可以从其他服务器正常读取数据。分布式文件系统在 Windows Server 2008 中集成在文件服务中，因此，为了使用 DFS 需要在服务器安装文件服务。

1. 安装文件服务器

在 Windows Server 2008 中，文件服务器的安装主要是通过采用完全向导的方式来完成。在安装过程中，用户可以完成服务器的一些基本设置和安装所需的组件。需要注意的是，在图 5-100 所示的“选择角色服务”对话框中，需要选中“分布式文件系统”复选框，具体操作步骤参见相关内容，这里就不再赘述。另外，在安装文件服务过程中，不要配置 DFS 命名空间。

2. 配置 DFS 群集

故障转移群集中配置 DFS 群集与配置 DHCP 服务器的操作相似，这里仅介绍不同的操作步骤。

(1) 在“故障转移群集管理”窗口中，右击“服务和应用程序”按钮，并在快捷菜单中选择“配置服务或应用程序”命令，显示“开始之前”对话框。

(2) 单击“下一步”按钮，显示图 5-101 所示的“选择服务或应用程序”对话框。在“选择要配置为高可用性的服务或应用程序”列表中，选择“DFS 命名空间服务器”选项。需要注意的是，当选择“DHCP 服务器”选项时，“下一步”按钮并不会立即显示为可用状态，此时向导会检查故障转移群集的相关配置，当检查通过后该按钮才会显示为可用状态。

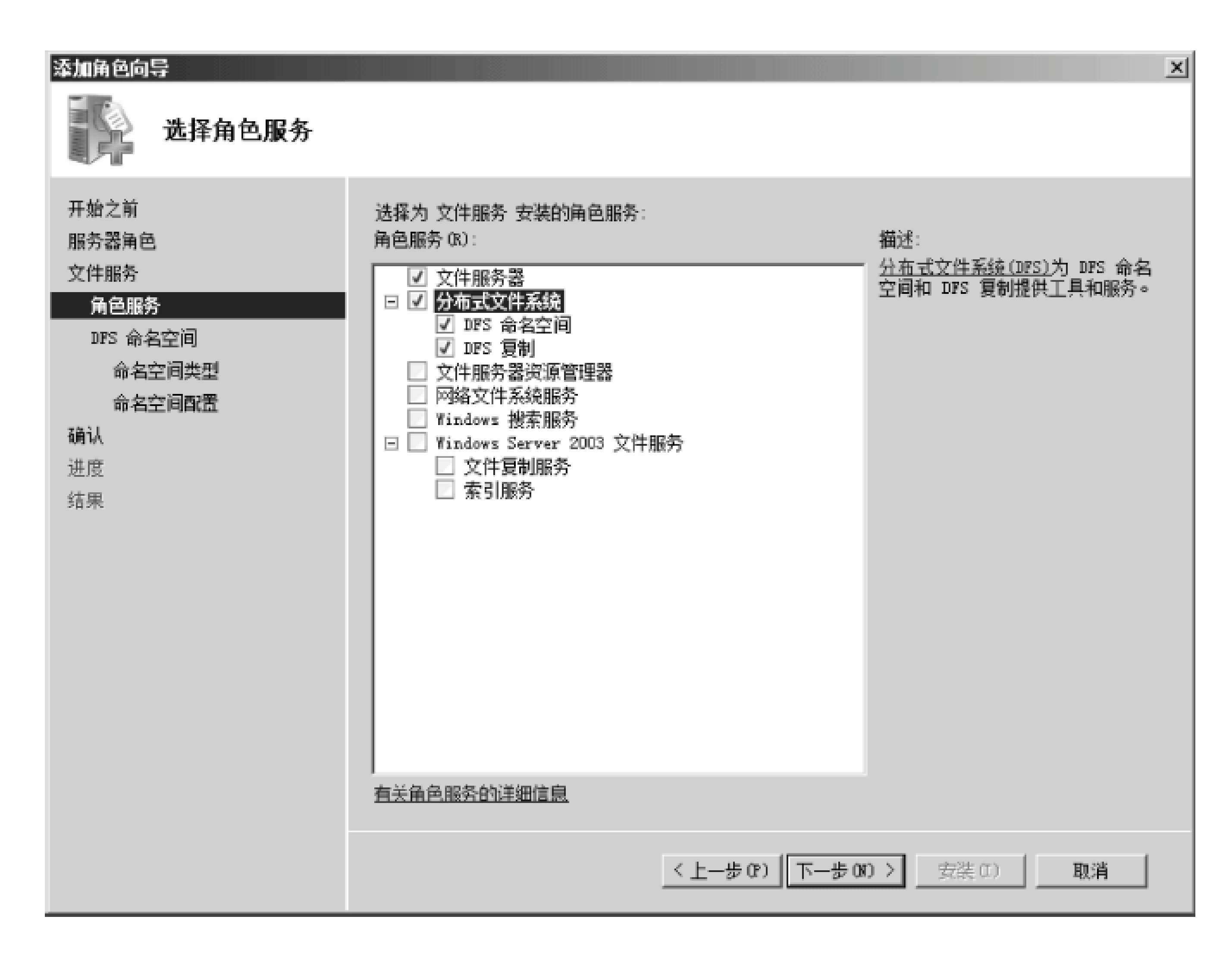


图 5-100 “选择角色服务”对话框



图 5-101 “选择服务或应用程序”对话框

(3) 单击“下一步”按钮，显示图 5-102 所示的“客户端访问点”对话框。在“名称”文本框中输入客户端用户访问的 DFS 名称。在“地址”文本框中输入客户端用户访问的服务器 IP 地址。

(4) 单击“下一步”按钮，显示“选择存储”对话框，选择所要使用的群集磁盘。

(5) 单击“下一步”按钮，显示图 5-103 所示的“DFS 信息”对话框。在“命名空间名称”文本框中输入 DFS 命名空间的名称。

(6) 单击“下一步”按钮，显示图 5-104 所示的“确认”对话框。显示该命名空间的详细信息，包括共享、路径、存储、网络名称和 IP 地址。

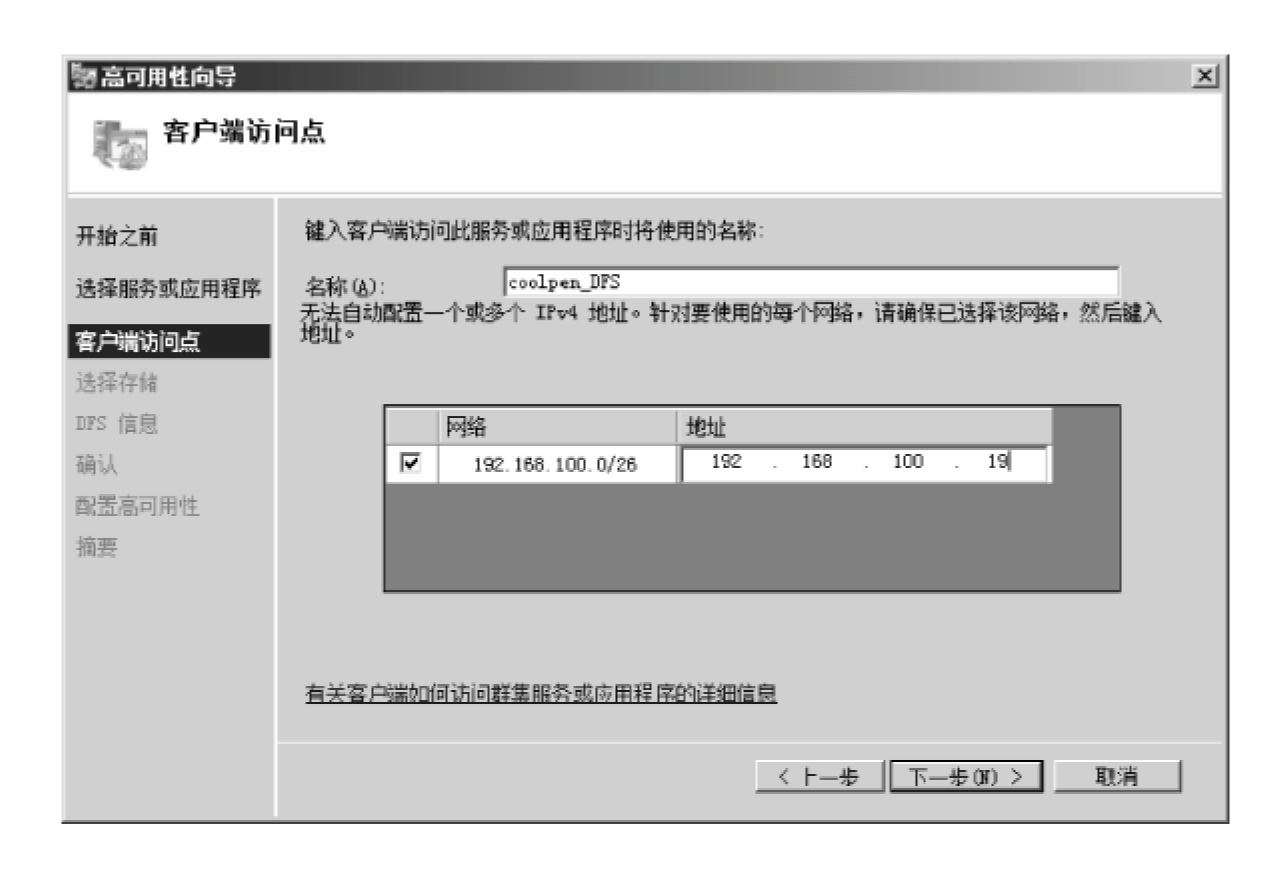


图 5-102 “客户端访问点”对话框

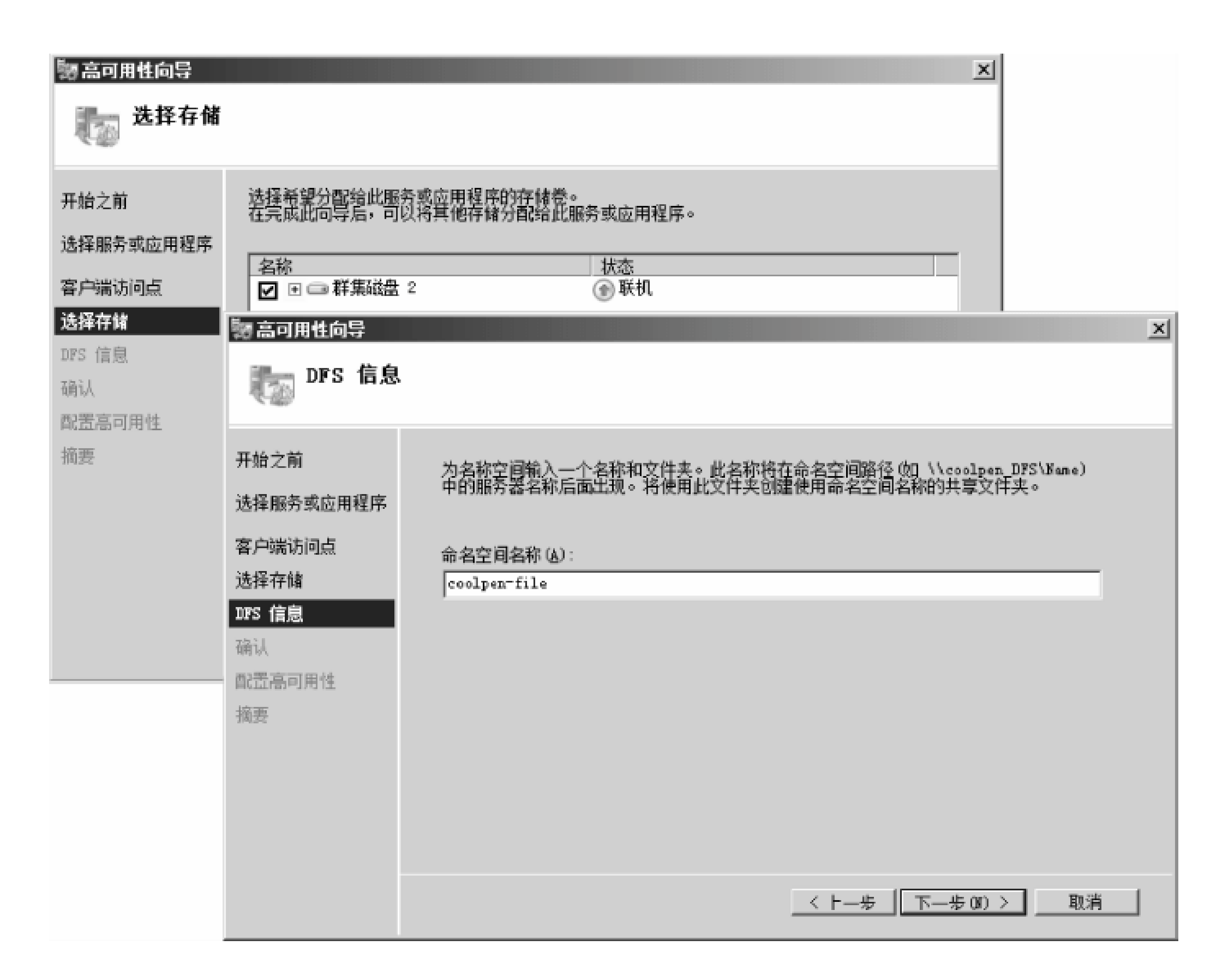


图 5-103 “DFS 信息”对话框



图 5-104 “确认”对话框

（7）单击“下一步”按钮，开始配置 DFS 命名空间服务器。配置完成后，显示图 5-105 所示的“摘要”对话框。



图 5-105 “摘要”对话框

（8）单击“完成”按钮，完成 DFS 文件分布式系统的配置，如图 5-106 所示。

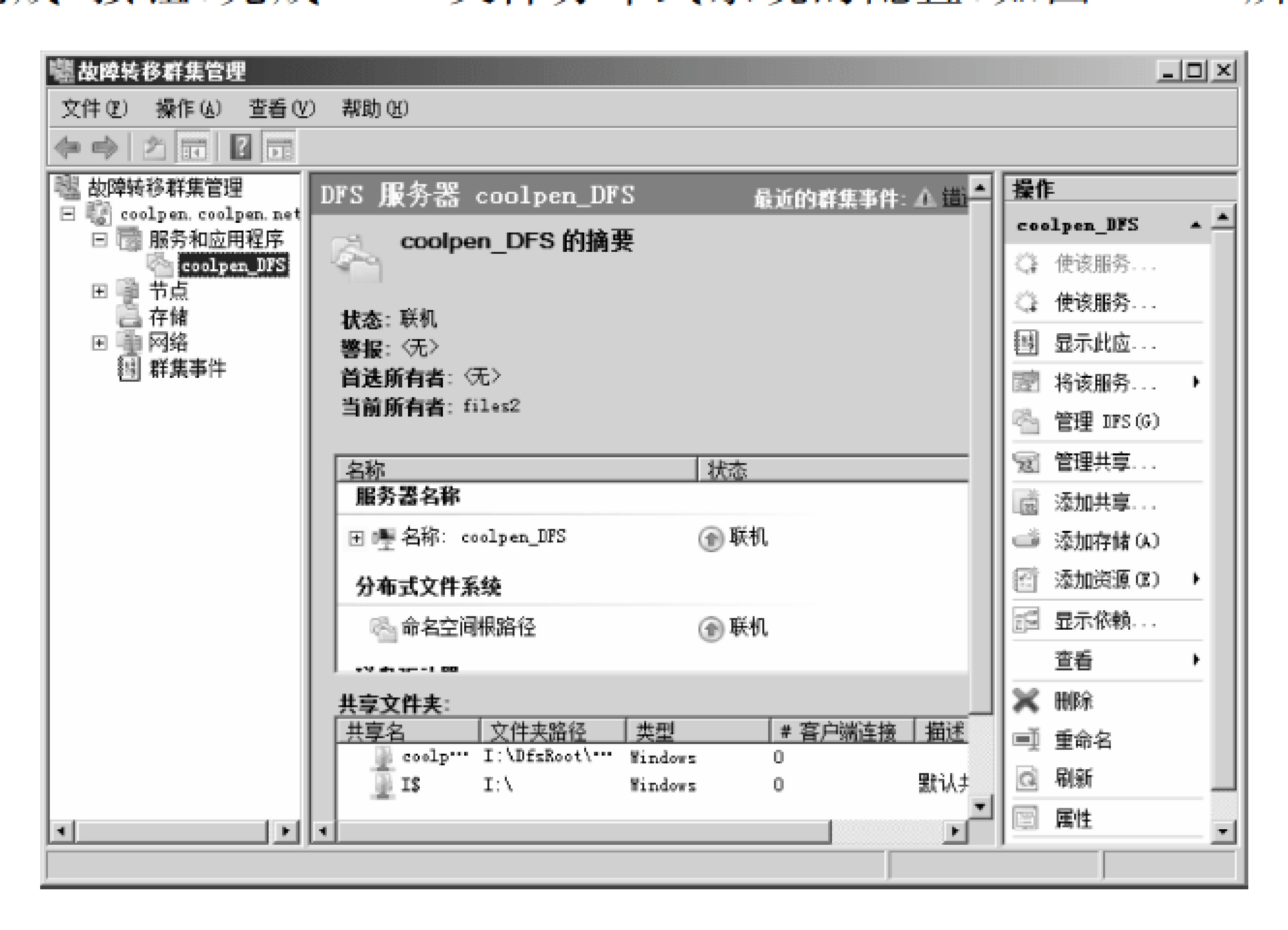


图 5-106 完成 DFS 文件分布式系统的配置

3. 管理 DFS

在故障转移群集中，管理 DFS 不能使用原有的“DFS 管理器”进行管理，需要通过使用群集的“DFS 管理”窗口来实现。这里以新建文件夹为例进行介绍。

（1）在“故障转移群集管理”窗口中，单击“管理 DFS”按钮，打开“DFS 管理”窗口。

（2）在右侧“操作”栏中，单击“新建文件夹”按钮，显示图 5-107 所示的“新建文件夹”对话框，在“名称”文本框中输入文件夹名，这里设置为 software。

（3）单击“添加”按钮，显示“添加文件夹目标”对话框。

（4）单击“浏览”按钮，显示图 5-108 所示的“浏览共享文件夹”对话框。单击“浏览”按钮，显示“选择计算机”对话框，在“输入要选择的对象名称”文本框中输入计算机名称，然后单击“确定”按钮。在“浏览共享文件夹”对话框中，从“共享文件夹”列表中选择欲添加的共享文件夹。重复操作可添加多个文件夹。

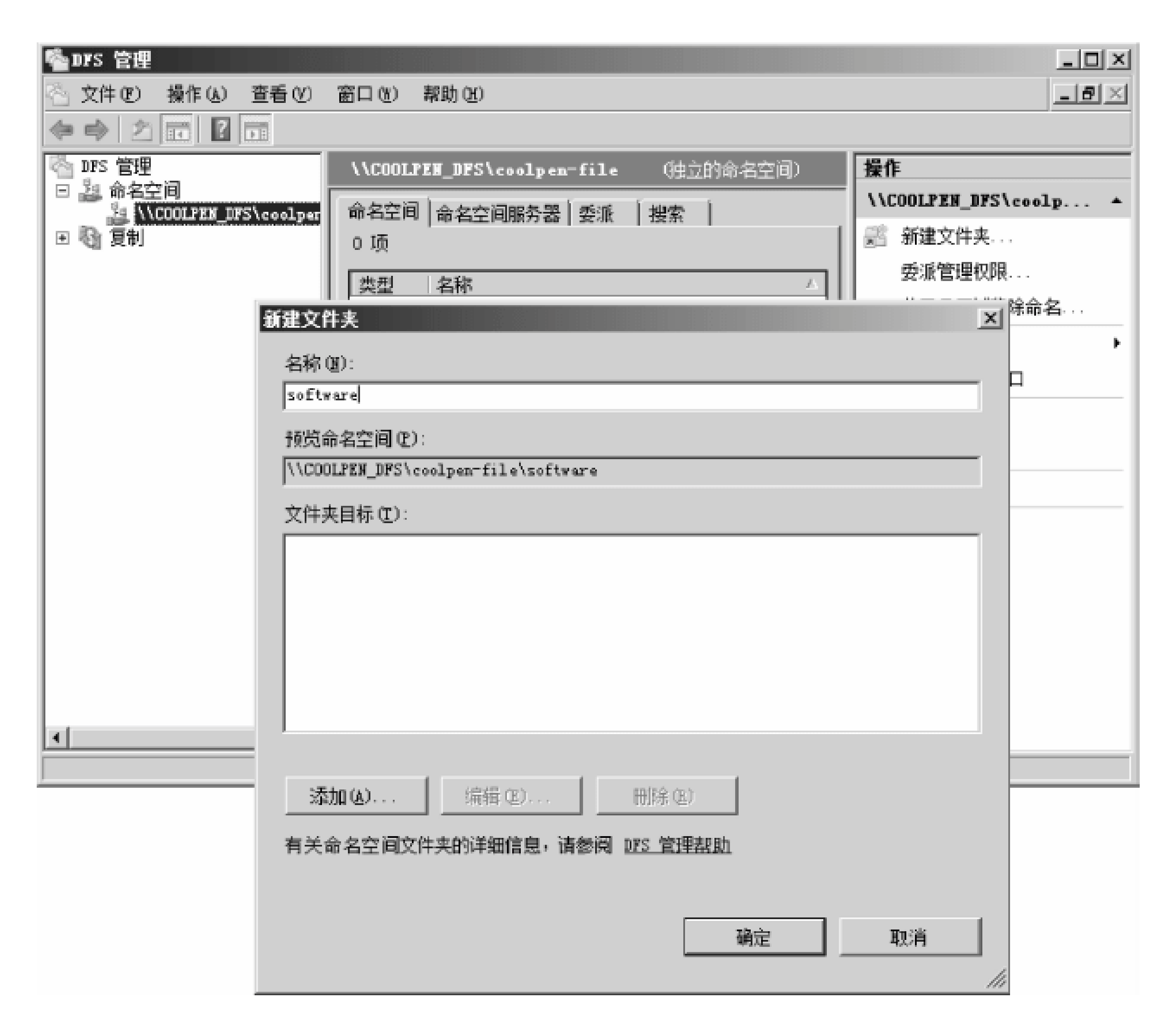


图 5-107　“新建文件夹”对话框



图 5-108　“浏览共享文件夹”对话框

（5）依次单击“确定”按钮，完成文件夹的创建，如图 5-109 所示。

4．DFS 文件系统群集测试

支持 DFS 的客户端有 Windows 9x/2000/Me/XP/2003/Vista/2008 等操作系统，客户端可以访问 DFS 内的文件。可以在客户端计算机上使用“\\服务器名或 IP 地址\根目录”的方式来访问 DFS 资源。

在资源管理器任务栏中，输入\\coolpen_DFS，按 Enter 键确认，即可访问该共享，如图 5-110 所示。需要注意的是，当从网络中访问时可能需要用户提供具有访问权限的用户信息。



图 5-109　完成文件夹的创建



图 5-110　访问共享

5.6　网络负载平衡

Windows Server 2008 中的网络负载平衡(NLB)功能可以增强 Internet 服务器应用程序的可用性和可伸缩性,例如 Web 服务器、FTP 服务器、防火墙、代理服务器、虚拟专用网络(VPN)以及其他执行关键任务的服务器上使用的应用程序。

5.6.1　网络负载平衡规划

网络负载平衡是将网络连接客户与服务器应用分布在同一个 NLB 群集内的多个服务器上。可以使用户在访问应用时,通过网络负载平衡决定由哪台服务器响应,从而实现分担服务器负担。

在本书的网络环境中,由于 Web 服务器的访问量比较大,因此部署两台 Web 服务器,并部署网络负载平衡。其中,两台服务器的 IP 地址分别设置为 192.168.100.7 和 192.168.100.8,网络负载平衡后所使用的 IP 地址为 192.168.100.10。

5.6.2 网络负载平衡的连接

目前,基本所有的服务器都会集成两块以上的网卡,使服务器可以同时连接两个不同的网络,如图 5-111 所示。

1. 设置网卡属性

在每个节点采用相同的方式安装和配置网卡。通常情况下,每个节点的每块网卡的所有属性都应当设置为相同值,例如,网卡应当设置为网络的实际速度,而不要将网卡设置为自适应,自动检测网络速度。如果允许网卡检测速度,一些网卡会在判断速度时丢弃网络数据包。所有其他网络属性,如双工模式、流控制和媒体类型,也应当设置为相同值。

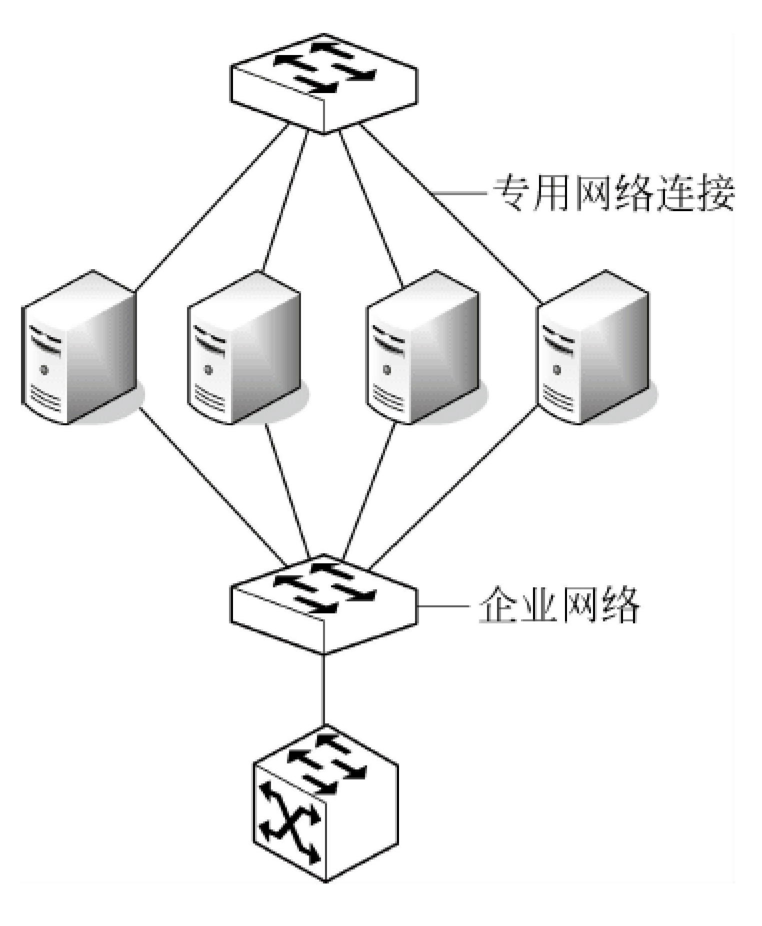


图 5-111 群集的网络连接

2. 选择网络协议

所有网卡都必须取消对 NetBIOS over TCP/IP 选项(位于 WINS 选项卡)的选择,并且使 TCP/IP 协议成为连接专用网络网卡的唯一网络协议。

3. 设置 IP 地址信息

正确设置专用和公用 IP 地址信息,不仅对支持客户端请求至关重要,而且群集服务也使用这些设置在节点之间发送群集的运行情况。公用网卡响应客户端对群集中网络服务的请求,因此,应当使用与企业网络相关的 IP 地址。专用适配器只用于节点间的通信,因此,建议使用保留的私有 IP 地址。不要使用 DHCP 为任何网卡分配 IP 地址,而应当为所有网卡指定静态 IP 地址信息。为公用网卡和虚拟服务器选择的 IP 地址,必须在企业网络的范围内,并被客户端所访问。

5.6.3 安装网络负载平衡

在安装网络负载平衡前,必须配置使安装 NLB 的适配器上只有 TCP/IP 协议,不能向该适配器中添加任何其他协议(例如 IPX)。NLB 可以将 TCP/IP 协议用作其网络协议,并且与特定的传输控制协议(TCP)或用户数据报协议(UDP)端口相关联的任何应用程序或服务进行负载平衡。

(1) 依次选择“开始”→“管理工具”→“服务器管理器”命令,打开图 5-112 所示的“服务器管理器”窗口。在左侧栏中,选择“功能”选项。

(2) 在右侧“功能”窗口中,单击“添加功能”链接,显示图 5-113 所示的“添加功能向导”对话框。在“功能”列表中,选中“网络负载平衡”复选框。

(3) 单击“下一步”按钮,显示“确认安装选择”对话框。

(4) 单击“安装”按钮,即可开始安装网络负载平衡,安装完成后,显示图 5-114 所示的“安装结果”对话框。

(5) 单击“关闭”按钮,完成网络负载平衡的安装。此时,即可通过使用网络负载平衡管理器配置 NLB 群集。

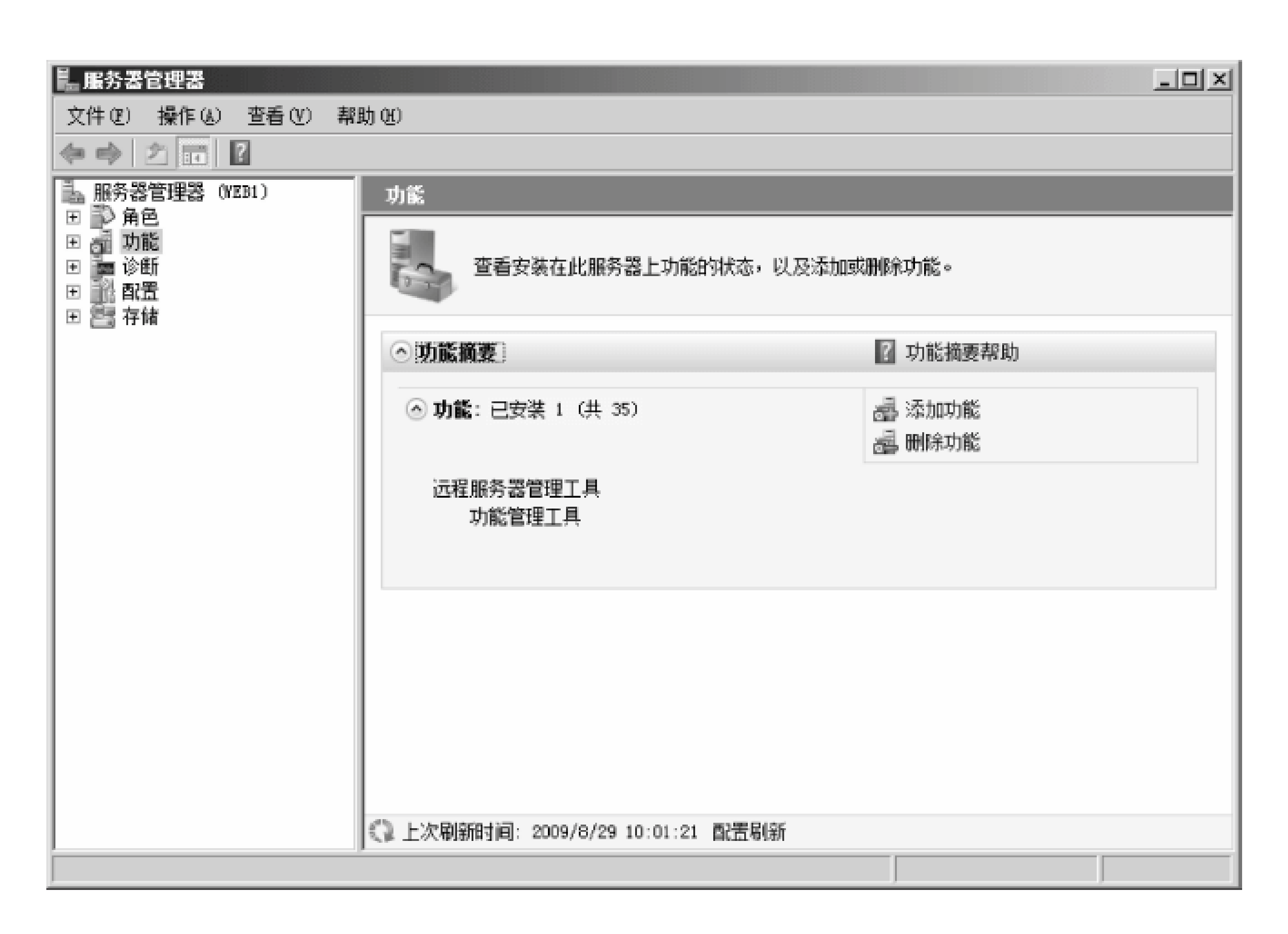


图 5-112 “服务器管理器”窗口



图 5-113 “添加功能向导”对话框

5.6.4 创建网络负载平衡群集

使用网络负载平衡管理器时,必须是正在配置的主机上的 Administrators 组的成员,或者被委派了适当的权限的用户。如果通过不属于群集的计算机运行 NLB 管理器来配置群集或主机,则不必是该计算机 Administrators 组的成员。

1. 新建网络负载平衡群集

依次选择“开始”→“管理工具”→“网络负载平衡管理器”命令,即可启动网络负载平衡管理器。

(1) 右击“网络负载平衡群集”选项,在快捷菜单中选择“新建群集”命令,显示“新群集:连接”对话框。在“主机”文本框中输入欲添加的主机的 IP 地址。单击“连接”按钮,即可开



图 5-114　“安装结果”对话框

始连接到群集计算机，如图 5-115 所示。在“可用于配置新群集的接口”列表中，显示该主机可用的网络连接，并选择所要使用的网络连接接口。



图 5-115　成功连接到远程主机

(2) 单击“下一步”按钮，显示图 5-116 所示的“新群集：主机参数”对话框。在“优先级(单一主机标识符)”下拉列表框中，选择所要使用的某个值。该参数为每个主机指定一个唯一 ID。在“默认状态”下拉列表框中，可以选择设置完成后该群集的状态，默认选择“已启动”选项。如果选中“在计算机重新启动后保持挂起状态”复选框，可以在群集计算机重新启

动后保持挂起状态，直到管理员手动启动。

（3）单击“下一步”按钮，显示“新群集：群集 IP 地址”对话框。在该对话框中，根据需要设置群集的每个成员所共享的群集 IP 地址，即负载平衡时所使用的 IP 地址。

（4）单击“添加”按钮，显示图 5-117 所示的“添加 IP 地址”对话框。因为这里只使用 IPv4 地址，所以只能选中“添加 IPv4 地址”单选按钮。在“IPv4 地址”和“子网掩码”文本框中，分别输入想要设置的 IP 地址和子网掩码。



图 5-116 “新群集：主机参数”对话框



图 5-117 “添加 IP 地址”对话框

（5）单击“确定”按钮，返回“新群集：群集 IP 地址”对话框，单击“下一步”按钮，显示图 5-118 所示的“新群集：群集参数”对话框。根据实际需要，设置 IP 地址和子网掩码，在“完整 Internet 名称”文本框中，输入用户将用于访问该 NLB 群集的 Internet 全名。在“群集操作模式”选项区域中，选择所要使用的群集操作模式，这里保持默认设置，即使用“单播”模式。在单播模式中，会将群集的 MAC 地址指定给计算机的网络适配器，不使用网络适配器的内置 MAC 地址。

（6）单击“下一步”按钮，显示图 5-119 所示的“新群集：端口规则”对话框。在该对话框中，可以根据需要修改端口规则，单击“编辑”按钮进行修改即可，这里保持默认设置。



图 5-118 “新群集：群集参数”对话框



图 5-119 “新群集：端口规则”对话框

(7) 单击“完成”按钮，完成设置。稍等片刻，即可成功创建群集，并将该主机添加到群集中，如图 5-120 所示。

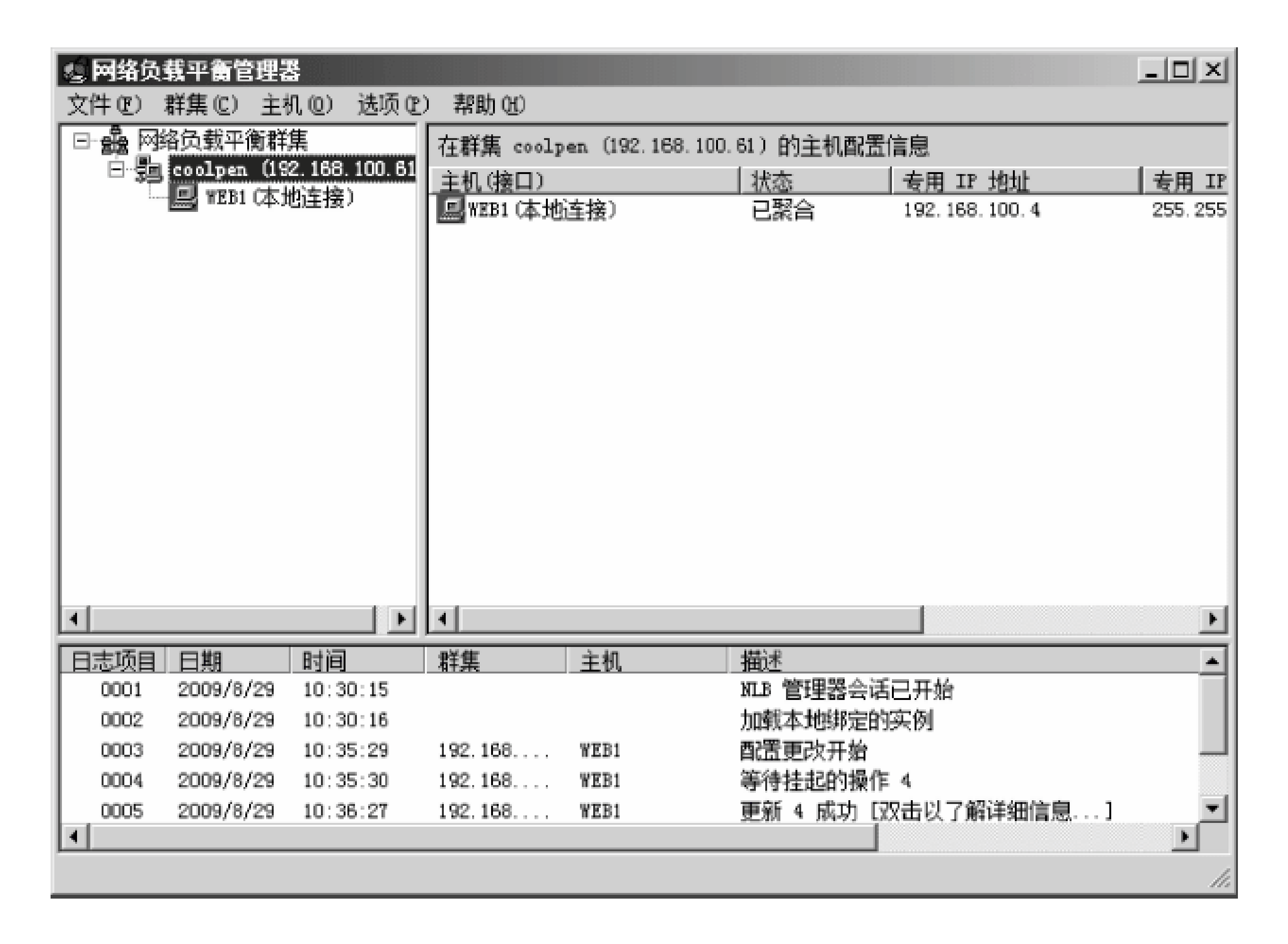


图 5-120 成功创建群集

2. 向群集中添加主机

通常情况下，群集的计算机可能会有多台，为了使所提供的服务更加稳定，可能会向群集中添加更多的主机。具体操作步骤如下。

(1) 在“网络负载平衡管理器”窗口中，右击群集名称，在快捷菜单中选择“添加主机到群集”命令，显示图 5-121 所示的“将主机添加到群集：连接”对话框。在“主机”文本框中输入想要添加的主机 IP 地址，单击“连接”按钮，即可连接到该主机。

(2) 单击“下一步”按钮，显示图 5-122 所示的“将主机添加到群集：主机参数”对话框。具体设置方法同新建网络负载平衡群集相同，这里就不再赘述。

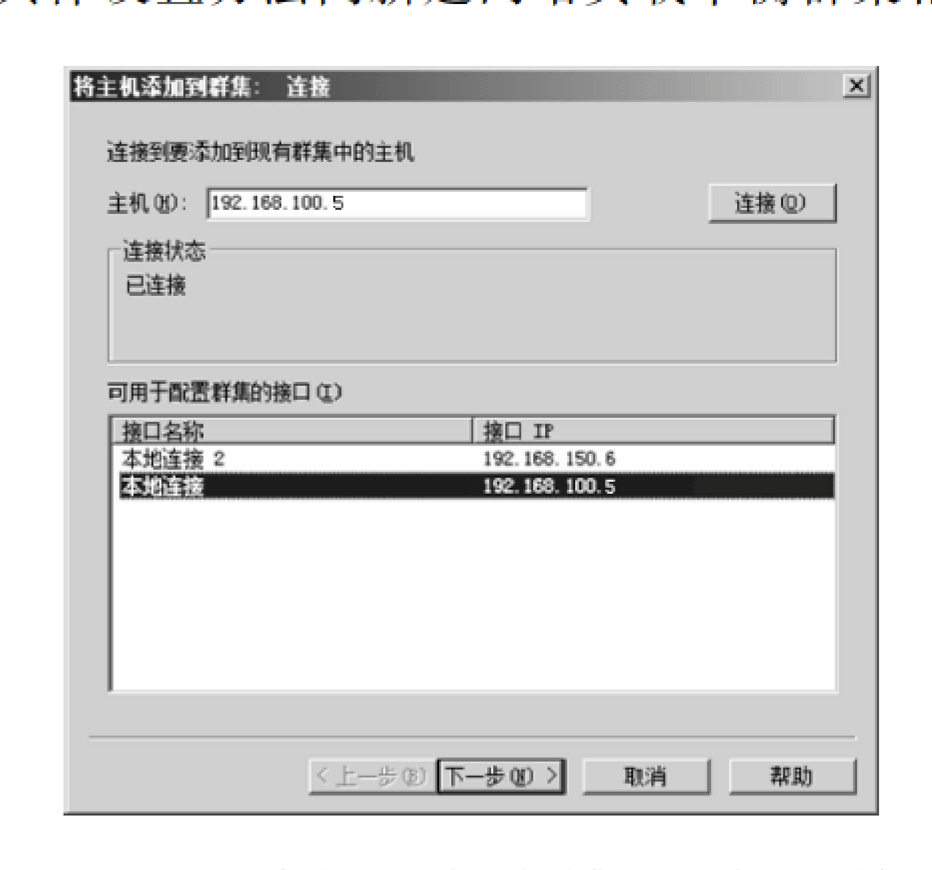


图 5-121 “将主机添加到群集：连接”对话框

图 5-122 “将主机添加到群集：主机参数”对话框

(3) 单击“下一步”按钮，显示图 5-123 所示的“将主机添加到群集：端口规则”对话框。根据需要进行设置即可，这里保持默认设置。

(4) 单击“完成”按钮，完成主机的添加，如图 5-124 所示。



图 5-123 “将主机添加到群集：端口规则”对话框

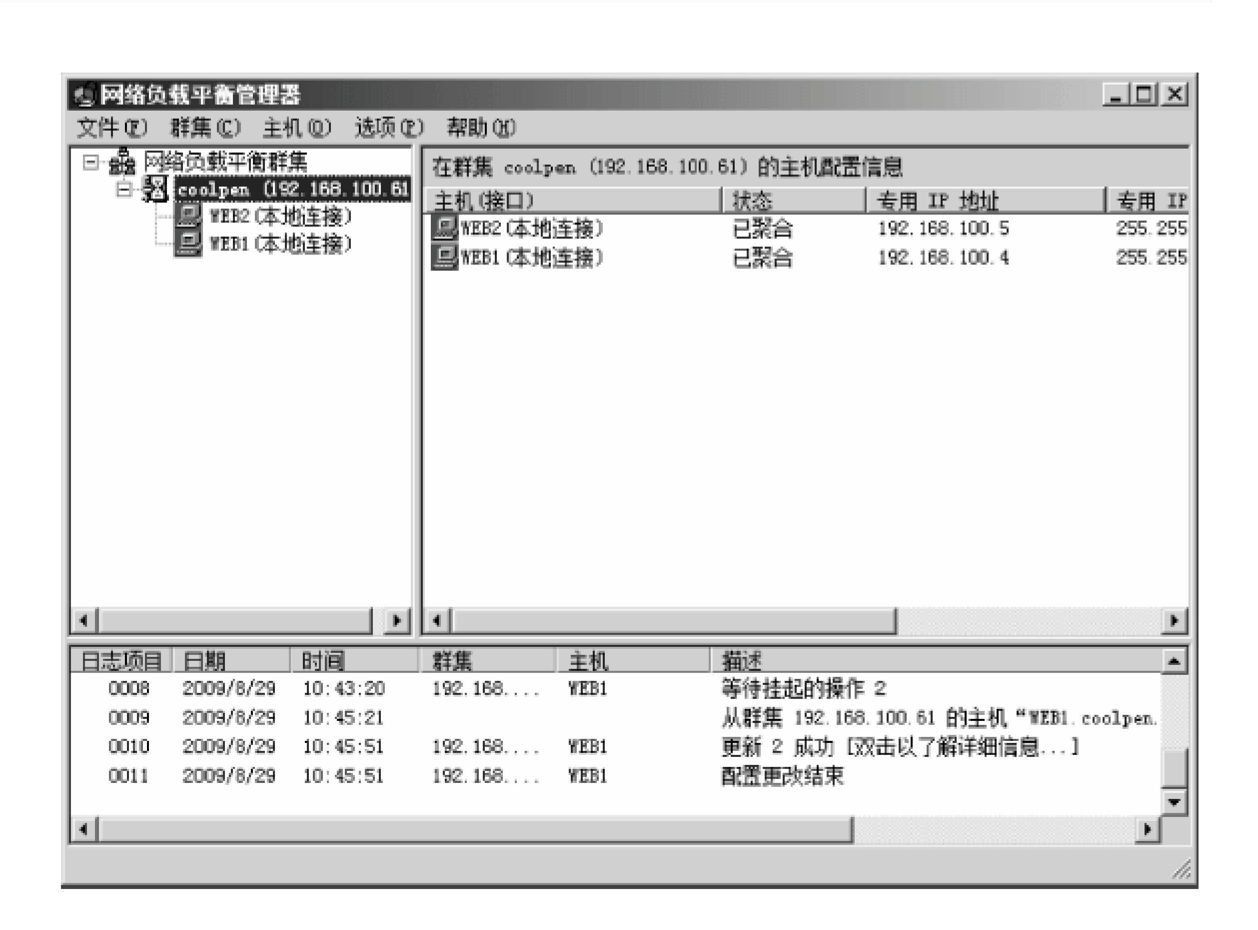


图 5-124 添加两台群集服务器

5.6.5 配置网络负载平衡群集

通常情况下，网络负载平衡需要根据不断的变化修改配置，例如，配置网络负载平衡的参数、配置网络负载平衡的工作模式、配置网络负载平衡的主机参数、编辑网络负载平衡的端口规则和配置网络负载平衡的日志设置。

1. 配置网络负载平衡群集参数

配置网络负载平衡群集参数时，只需在单个主机上进行配置。所有主机将自动继承初始主机中的群集配置，在“属性”对话框中设置的参数记录到每个主机的注册表中。

(1) 在“网络负载平衡管理器”窗口中，右击群集名称，在快捷菜单中选择“群集属性”命令，显示图 5-125 所示的群集属性对话框。选择“群集 IP 地址”选项卡，在“群集 IP 地址”列表中，选中所设置的虚拟 IP 地址，单击“编辑”按钮，打开“编辑 IPv4 地址”对话框，根据需要修改 IP 地址信息即可。也可单击“添加”按钮，添加其他群集 IP 地址。

(2) 单击“确定”按钮，保存设置。选择图 5-126 所示的“群集参数”选项卡，在“IP 地址”下拉列表框中，根据需要选择所要使用的群集 IP 地址。在“完整 Internet 名称”文本框中输入想要修改的群集名称。在“群集操作模式”选项区域，根据需要选择所需的模式。



图 5-125 群集属性对话框



图 5-126 “群集参数”选项卡

(3) 选择图 5-127 所示的“端口规则”选项卡，在该选项卡中的设置方法与前面所述相同，这里就不再赘述。

(4) 单击“确定”按钮，保存设置。

2. 配置网络负载平衡管理器日志设置

记录网络负载平衡管理器中的事件与记录 NLB 驱动程序生成的事件有所不同，NLB 管理器仅记录与使用 NLB 管理器有关的事件。若要查看与 NLB 驱动程序有关的事件，则需要使用“事件查看器”。

需要注意的是，应该始终从受信任且安全的计算机上管理 NLB 群集，尤其在启用事件日志记录时更应如此。NLB 管理器日志文件包含有关 NLB 群集和主机的潜在敏感信息，因此必须有适当的安全保护。默认情况下，日志文件继承创建其所在目录的安全设置。

在“网络负载平衡管理器”窗口中，依次选择“选项”→“日志设置”选项，显示图 5-128 所示的“日志设置”对话框。选中“启用日志”复选框，在“日志文件名”文本框中输入日志文件的名称。



图 5-127 “端口规则”选项卡

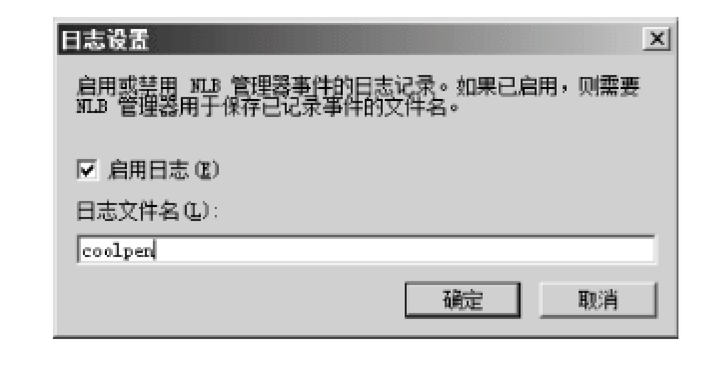


图 5-128 “日志设置”对话框

习题

1. 简述服务器群集的连接拓扑结构。
2. Windows 群集服务都有哪些软硬件要求？
3. 简述网络负载平衡连接拓扑结构。

实验：安装并配置 DFS 群集

实验目的：

掌握 Windows Server 2008 服务器的群集技术。

实验内容：

在企业中企业网络通过两台文件服务器，并使用 Windows Server 2008 所提供的群集，将两台服务器群集连在一起使用，以提高网络服务的稳定性。

实验步骤：

（1）将各服务器分别连接到局域网交换机的相应端口。

（2）在每个节点的计算机上安装 Windows Server 2008，并将每个节点均加入到域中。

（3）在两台服务器上部署存储服务。

（4）在 Windows 群集所有节点上安装群集服务。

（5）验证故障转移群集。

（6）创建故障转移群集。

（7）在各节点上安装文件服务器。

（8）配置 DFS 群集。

（9）管理 DFS 群集。

（10）测试 DFS 文件系统群集。

第 6 章 chapter 6

网络设备管理

网络设备主要是指交换机、集线器、路由器、防火墙等设备，是组建网络不可或缺的组成部分，其中交换机是最基本的网络设备。在早期的网络中，所使用的网络设备多为不可网管设备，例如通常所说的傻瓜交换机，可随着网络规模的不断扩大，以及网络应用的不断发展，所使用的网络设备的数量和种类也越来越多，为了满足网络的要求，可网管网络设备开始在网络中使用。使用可网管网络设备，能够使网络功能发挥到最大，并最大限度地保证网络的安全。

6.1 网络设备管理规划

网络设备是各种设备连接的基础，其中因为网络设备所处的位置的不同，设备的重要性也有所不同，但相同的是所有的设备都需要管理员进行管理。只有保证设备的正常运行，才能保证设备所连接的其他设备正常连接网络。

6.1.1 项目背景

在当前网络中，所有的网络设备，例如路由器、交换机、安全设备和无线设备等均使用 Cisco 的产品，并且所有的设备均使用可网管的网络设备，即所有设备均可进行配置，以实现不同的功能及应用。正因为在当前网络中所有的设备都是 Cisco 设备，因此，对于网络设备的管理实际上主要是管理 Cisco 产品。

6.1.2 项目需求

所有的可网管设备在出厂时都已经有初始配置，但这些配置是远远不能满足需求的，因此，管理员必须根据当前网络的要求对网络设备进行进一步配置。当进一步配置完成后，即可根据需要选择不同的管理方式，并可对网络设备进行备份和恢复等操作。另外，为了设备的安全运行，还应实时地对网络设备进行监控和配置。

6.1.3 解决方案

对于当前网络中设备的管理需求，可使用如下方案解决。

(1) 对于网络设备的初始配置通常可采用超级终端方式或 Web 方式实现，对于初始配置而言，Web 方式显然要比超级终端方式简捷方便。而对于日常管理，则可以选择超级终

端、Telnet、Web 和网管软件中的任何一种方式，此时所选择的管理方式的原则是方便、安全。

（2）当设备配置完成后，为了能够在设备发生故障或其他问题时使用相同的配置，可以将当前的配置文件进行备份，对于 Cisco 设备而言，可以在网络中安装 TFTP 服务器实现配置文件的备份与恢复。

（3）当设备的密码丢失时，无论是交换机还是路由器，都需要使用超级终端方式直接连接设备的 Console 端口完成。

（4）使用 CiscoWorks LMS 可以使网络管理人员通过 Web 页面的方式直观、方便、快捷地完成设备的配置、管理、监控和故障分析等任务。

6.2 网络设备管理方式与适用

因为网络设备通常没有键盘等输入设备，也没有显示器等输出设备，因此，需要借助其他方式对其进行管理。在购买到一台新设备时，首先需要使用超级终端对其进行基本设置，此后，即可使用 Telnet 或 SecureCRT 远程登录到设置上进行管理。另外，还可以通过使用 Web 方式和网管软件方式等进行远程管理。需要注意的是，在 Windows Vista 和 Windows Server 2008 中，默认不安装 Telnet 工具，需要手动安装。

6.2.1 超级终端方式

超级终端是 Windows 系统自带的一个程序，使用该程序可以连接到其他计算机、Telnet 站点、公告板系统(BBS)、联机服务和主机。在 Windows XP 系统中，默认已经安装了超级终端，而在 Windows Server 2003 系统下，则需要管理员手动安装该组件。

（1）依次选择“开始”→“控制面板”→“添加/删除程序”命令，打开图 6-1 所示的“添加或删除程序”对话框。

（2）在左侧栏中，单击“添加/删除 Windows 组件”按钮，显示图 6-2 所示的“Windows 组件向导”对话框。在“组件”列表中，选中“附件和工具”复选框。

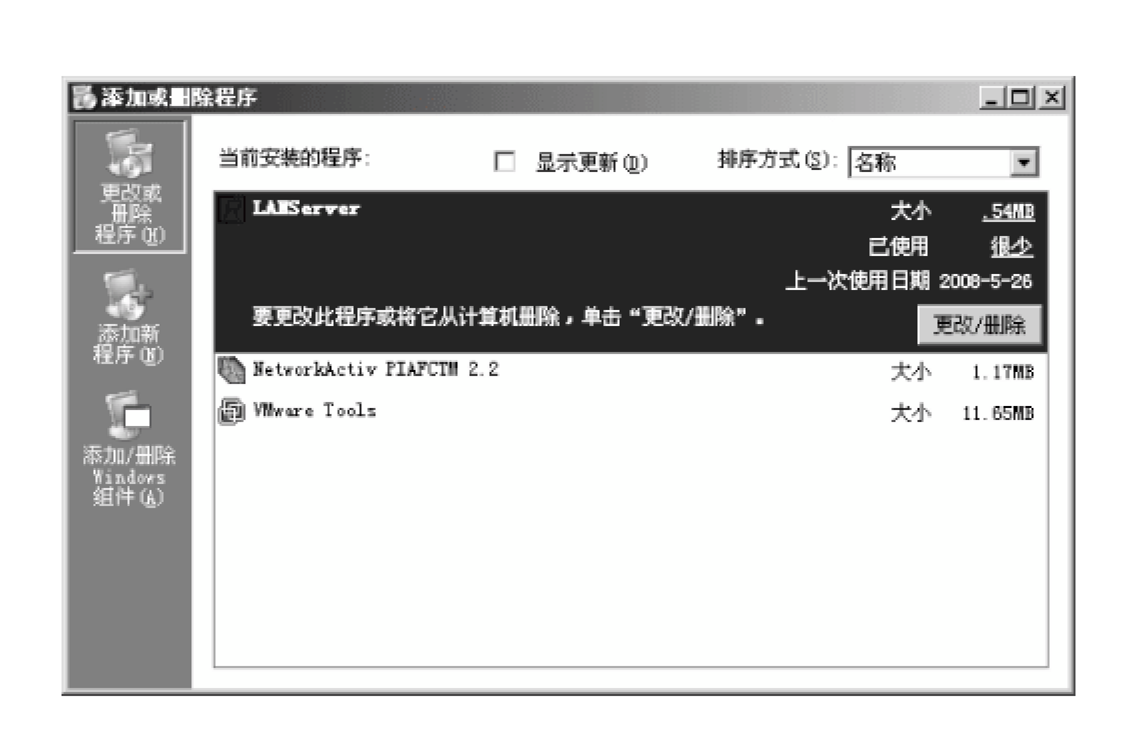


图 6-1 “添加或删除程序”对话框



图 6-2 “Windows 组件向导”对话框

（3）单击“详细信息”按钮，显示图 6-3 所示的“附件和工具”对话框。在“附件和工具 的子组件”列表中，选中“通讯”复选框。

（4）单击“详细信息”按钮，显示图 6-4 所示的“通讯”对话框。在“通讯 的子组件”列表中，选中“超级终端”复选框。

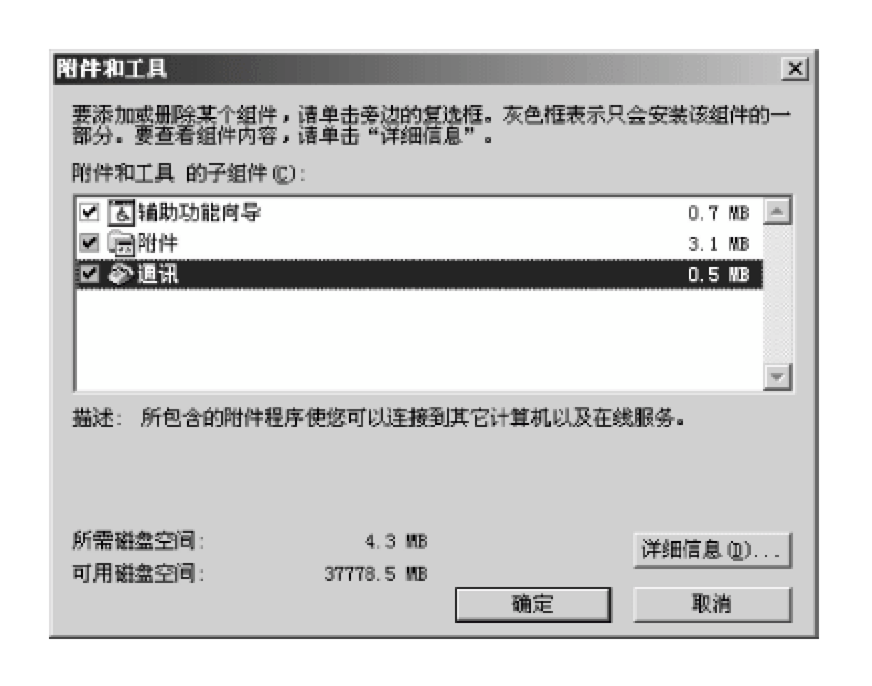


图 6-3　“附件和工具”对话框

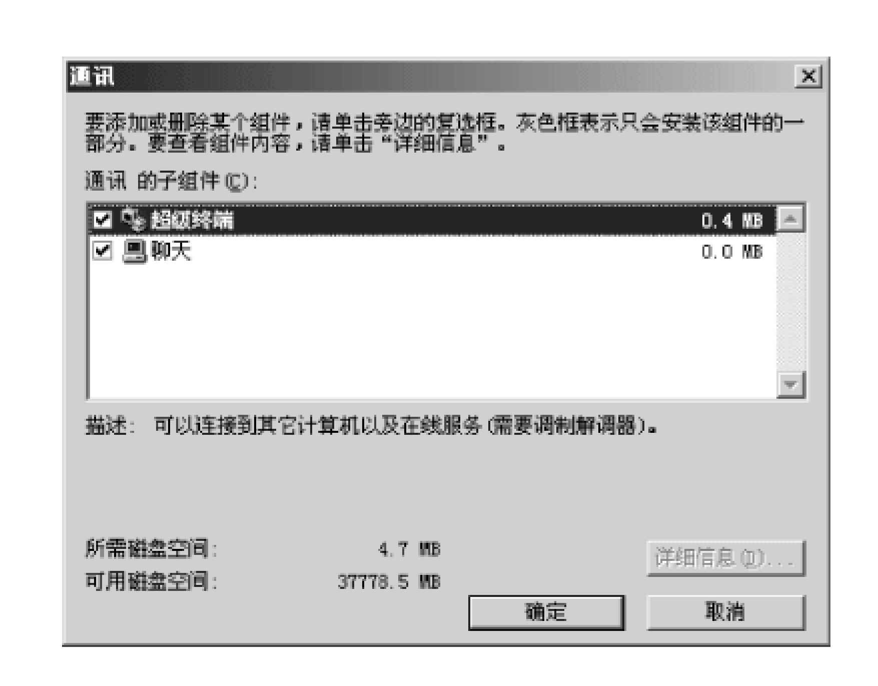


图 6-4　“通讯”对话框

（5）连续单击“确定”按钮，返回“Windows 组件向导”对话框，然后单击“下一步”按钮，即可将超级终端组件安装到计算机。需要注意的是，在安装过程中，需要用户插入 Windows Server 2003 安装光盘，才能正常安装完成。安装完成后，显示图 6-5 所示的“完成‘Windows 组件向导’”对话框。

（6）单击“完成”按钮，即可完成安装。

在使用超级终端建立与交换机的通信之前，必须先对超级终端进行必要的设置。

（1）依次选择“开始”→“所有程序”→“附件”→“通讯”→“超级终端”命令，显示图 6-6 所示的“默认 Telnet 程序”对话框。提示是否将超级终端作为默认 Telnet 程序，在这里根据实际需要进行设置即可。



图 6-5　“完成‘Windows 组件向导’”对话框



图 6-6　“默认 Telnet 程序”对话框

（2）单击“是”按钮，显示图 6-7 所示的“位置信息”对话框。在“目前所在的国家(地区)”下拉列表框中，选择“中华人民共和国”选项。在“您的区号(或城市号)是什么”文本框中，输入当前计算机所在的地区区号，例如 0311 代表石家庄。在“您拨外线需要先拨哪个号码”文本框中，输入需要设置的号码。

（3）单击“确定”按钮，显示图 6-8 所示的“电话和调制解调器选项”对话框。在该对话框中，显示了前面所进行的设置。

（4）单击“确定”按钮，显示图 6-9 所示的“连接描述”对话框。在“名称”文本框中输入该连接的名称，如 Cisco，用于标识与 Cisco 交换机的连接。





图 6-7 “位置信息”对话框

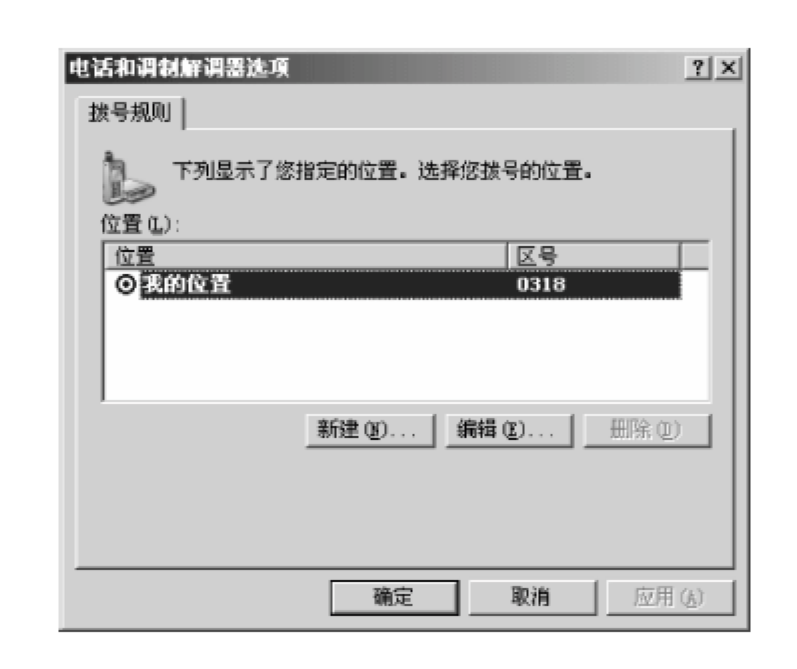


图 6-8 “电话和调制解调器选项”对话框

（5）单击“确定”按钮，显示图 6-10 所示的“连接到”对话框。在“连接时使用”下拉列表框中选择所使用的串行口，通常为 COM1。

（6）单击“确定”按钮，显示图 6-11 所示的“COM1 属性”对话框。在“每秒位数”下拉列表框中选择 9600，其他各选项采用默认值即可。



图 6-9 “连接描述”对话框

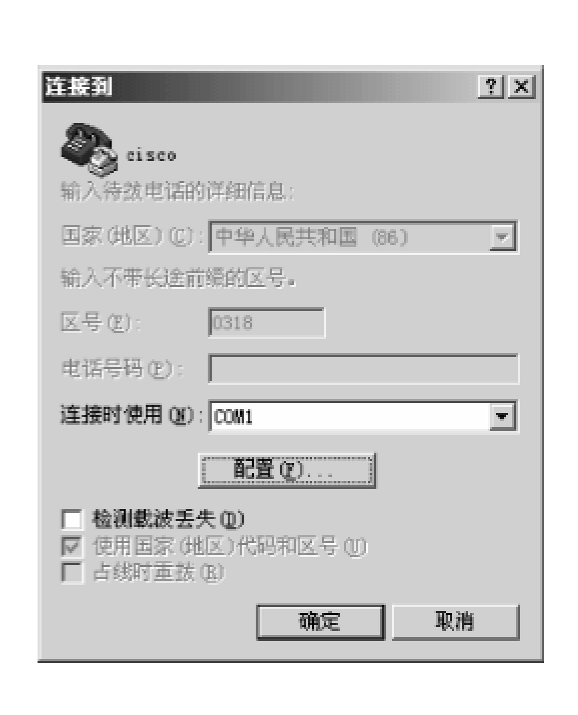


图 6-10 “连接到”对话框



图 6-11 “COM1 属性”对话框

注意：不同品牌的交换机和路由器对“数据流控制”参数的要求不同，例如华为产品为“无”，而 Cisco 产品则为“硬件”，因此，应当查看产品配置和使用手册。

（7）单击“确定”按钮，显示图 6-12 所示的“cisco-超级终端”窗口。

（8）打开交换机电源后，连续按 Enter 键，即可显示交换机初始界面。图 6-13 所示为 Cisco 4006 交换机初始页面。



图 6-12 “cisco-超级终端”窗口

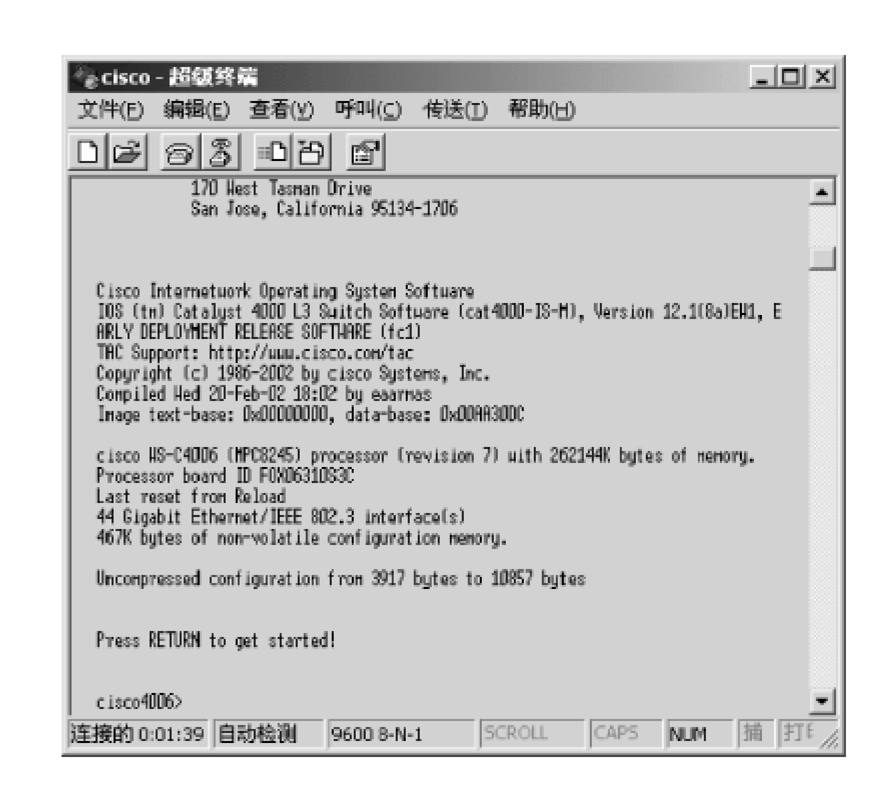


图 6-13 Cisco 4006 交换机初始页面

计算机与交换机连接成功之后，就可以以菜单(Menus)方式或命令行(Command Line)方式对交换机进行配置和管理了。

注意：如果在计算机屏幕上未能显示交换机的启动过程，则可能是通信端口选择错误，需重新配置超级终端。当然，也有可能是Console线或连接有问题，应当逐一进行检查。

6.2.2　Telnet方式

Telnet是集成在Microsoft TCP/IP协议中的一项网络服务，利用Telnet协议为虚拟终端提供一个标准的端口，用户不必了解终端设备的详细信息即可建立连接，另外，Telnet还为用户和终端设备提供一个协商选项的机制和一组标准选项。目前大多数网络设备的管理和配置都是通过这种方式进行的，如网络服务器的更新、路由器的配置、网络防火墙的配置等。

1. Telnet的工作过程

Telnet程序主要包括Telnet客户端程序和Telnet服务器程序两部分，分别运行于本地计算机和远程终端设备上。

其中，本地计算机上的Telnet客户端程序主要完成如下功能。

(1) 建立本地计算机与服务器端的TCP连接。

(2) 接收由本地计算机键盘输入的信息，并转换成标准格式发送给远程服务器端。

(3) 从远程服务器接收输出的信息。

(4) 将信息显示在本地计算机的屏幕上。

远程终端上的服务器端主要负责完成如下功能。

(1) 通知发送请求信息的计算机，终端设备已经准备就绪，等待输入命令。

(2) 执行输入的命令，如显示目录内容或执行某个应用程序等。

(3) 将执行命令的结果送回到主机的输出设备上。

(4) 等待执行新的命令。

通过使用Telnet程序，可以很轻松地在远程终端上完成网络设备的管理与配置，从而减少了很多管理网络设备的麻烦。

2. Telnet的常用参数

Telnet命令最多的应用是直接使用“Telnet＋远程主机名”或“Telnet＋IP地址”连接到对方默认的端口上，而很少应用各种参数选项，其实Telnet命令也是拥有多个用于实现不同功能的可选参数的，通过输入telnet-? 命令查看常用参数，如图6-14所示。

3. Windows Vista/2008安装Telnet组件

在Windows Vista/2008系统中，默认情况下，Telnet组件并没有随系统安装到计算机上，如果此时使用Telnet客户端程序，将显示图6-15所示的窗口。提示Telnet不是内部或外部命令，即需要用户安装该组件。

在Windows Vista安装Telnet组件，具体的操作步骤如下。

(1) 依次选择“开始”→“控制面板”命令，显示图6-16所示的“控制面板”窗口。

(2) 双击“程序和功能”图标，显示图6-17所示的“卸载或更改程序”窗口。在该窗口中，显示了当前计算机中所安装的所有程序。




图 6-14 Telnet 常用参数



图 6-15 默认不能使用 Telnet 程序



图 6-16 “控制面板”窗口

（3）在左侧栏中，单击“打开和关闭 Windows 功能”按钮，显示图 6-18 所示的“Windows 功能”窗口。在功能列表中，选中“Telnet 客户端”复选框，即安装 Telnet 客户端。





图 6-17 “卸载或更改程序”窗口

图 6-18 “Windows 功能”窗口

（4）单击“确定”按钮，即可安装并配置 Telnet 客户端。

注意：与 Windows Vista 所不同的是，在 Windows 2008 系统下安装 Telnet 组件，需要在“服务器管理器”窗口的添加功能列表中，添加 Telnet 组件。

4. 利用 Telnet 实现远程登录

虽然安装了 TCP/IP 协议就相当于安装了 Telnet 服务，但是在 Windows 系统中该服务是默认被禁止运行的，所以如果是使用 Telnet 远程管理网络服务器就必须先启动该项系统服务，或者使用其他已经开放的端口也可以（Telnet 默认使用 23 端口，并且该端口是关闭的）。

首先在本地计算机上打开命令提示符窗口，输入如下命令：

```
telnet 172.16.100.1
```

按 Enter 键运行，即可显示图 6-19 所示的连接界面，提示输入登录到远程主机的有效用户名和密码。由于是维护远程主机的系统信息，可使用系统管理员的用户名登录，以获得更高的配置权限。如果登录到的是远程交换机或者路由器，使用系统默认的用户名和密码即可。另外，在输入登录密码时应特别注意：在输入密码时，不会以任何形式显示，就好像根本没有输入任何字符一样，所以应尽量保证输入的准确性。Telnet 最多允许用户尝试登录 10 次，超出 10 次则自动断开与远程主机的连接。

提示：输入用户名之后按 Enter 键即可开始输入登录密码，再次按 Enter 键即可尝试登录。

成功登录到远程主机后，显示图 6-20 所示的界面，现在就可以像在对方系统中一样进行操作了，可以执行各种系统命令、启动/关闭应用程序、传输文件等，如果登录用户名拥有足够的权限，还可以关闭、注销或者重新启动远程主机。

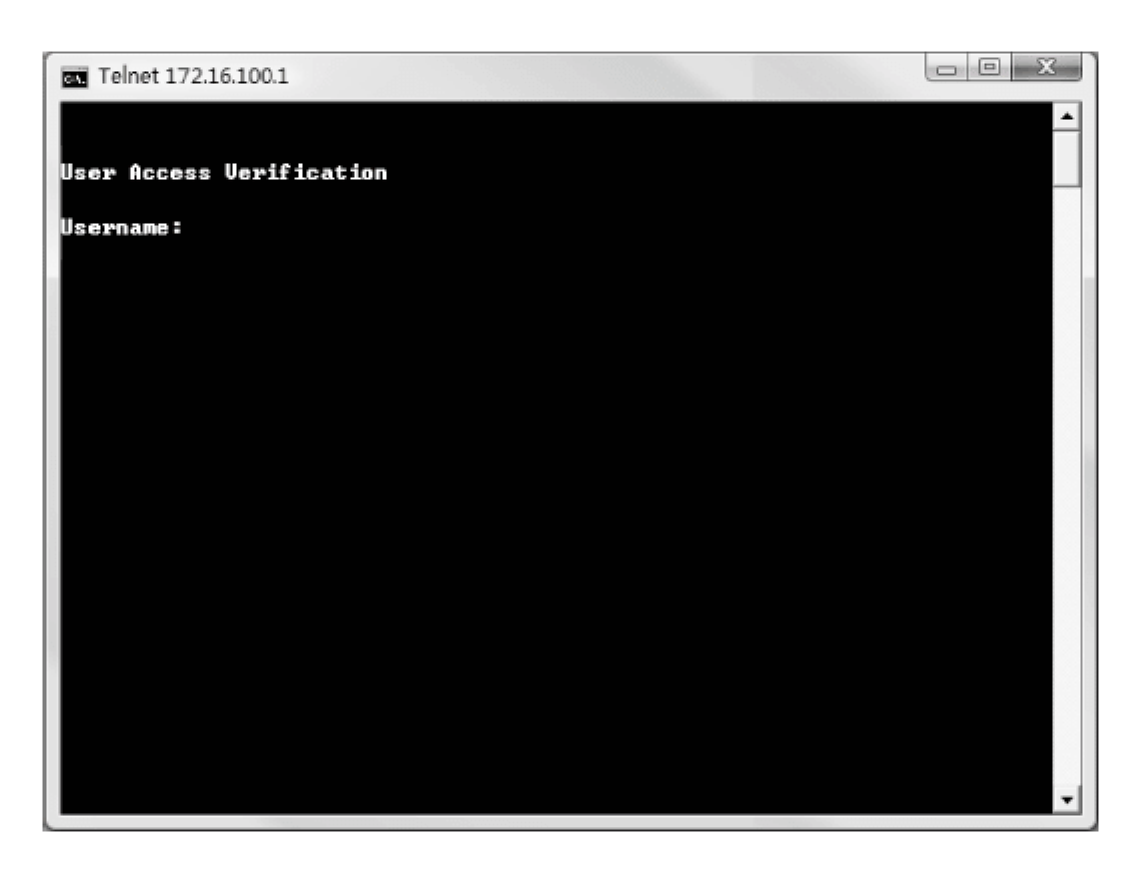


图 6-19　登录远程主机



图 6-20　登录成功

5. Telnet 的主要功能

借助 Telnet 登录到远程终端只是达到目的过程中的一个重要环节，利用 Telnet 可以实现对远程终端设备系统信息查看、配置信息查看、备份和恢复设置系统等内容。

（1）查看系统信息

查看网络设备系统信息是最基本的操作，也是必须掌握的技术，在对网络设备进行配置前，首先要了解设备本身的一些重要系统信息，例如登录到远程服务器，首先要查看该服务

器的一些详细信息，操作系统版本(使用 type c:\boot.ini 命令即可)、系统配置、安装了什么软件或服务等，只有这样才能发现系统究竟存在哪些漏洞，需要做什么进一步处理。如果是登录到远程路由器或者交换机，则会自动显示其系统信息，包括其当前设备类型、名称、生产厂家、操作系统版本等。

(2) 使用 TFTP 传输文件

传输文件是管理远程网络设备的一项重要工作，例如远程路由器的配置信息需要经常备份和更新，都是通过 Telnet 将配置好的信息备份到本地计算机上，出现问题需要恢复时再通过 Telnet 传输过去。

用 TFTP(Trivial File Transfer Protocol)传送文件是一种基于 UDP 连接的文件传输方式，一般是使用 Windows 自带的 tftp.exe 和一个 TFTP 服务器端软件(可以到 Internet 下载，许多都是免费的)构成一个完整的传输结构。首先将需要传输的配置文件保存到 TFTP 服务器软件所在的目录下，然后运行本地的 TFTP 服务器端(比如 tftpd32.exe)软件并保证始终开启直至传输全部完成。接着在登录成功的 Telnet 窗口中，执行图 6-21 所示的命令，即可查看 TFTP 命令的帮助信息。



图 6-21 传输文件

提示：TFTP 命令的完整格式如下。

TFTP [-i] [host] [{GET | PUT}] [source] [destination]

各参数的含义如下。

① -i：指定二进制图像传送模式(也称为八进制模式)。在二进制图像模式下，文件以一个字节为单位进行传输，在传送二进制文件时使用该模式。如果省略了-i，文件将以默认的 ASCII 模式传送。该模式将行尾(EOL)字符转换为指定计算机的适当格式，传送文本文件时使用该模式，如果文件传送成功，将显示数据传输速率。

② host：指定本地计算机或远程计算机，注意本例中应当是本地主机地址。

③ GET：将远程计算机上的文件传送到本地计算机指定的目录下。由于本例中已经使用 Telnet 登录到了远程终端，相当于在远程终端设备上操作，所以使用 GET。

④ PUT：将本地计算机上的文件传输到远程终端中，由于 TFTP 协议不支持用户身份验证，所以用户必须使用 Telnet(或其他方式)登录到远程计算机，并获取一定的控制权限。

⑤ source：指定要传送的文件。

⑥ destination：指定将文件送达的位置，如果省略了 destination，将假定它与 source 具有相同名称。

注意：如果使用代理服务器，将不能实现与外部网络的文件传送。因为代理网关在进行数据封装的时候会自动将自己的 IP 地址加入到数据报中，代替内部网络地址，所以在外部网络进行 MAC 寻址时是找不到正在运行的 TFTP 服务器的，因此造成传输失败。

6.2.3 Web 方式

当使用 Console 端口为交换机设置好 IP 地址信息并启用 HTTP 服务后，即可通过支持 Java 的 Web 浏览器访问交换机，并可通过 Web 浏览器修改交换机的各种参数并对交换机进行管理。与 Telnet 冷冰冰的纯字符界面相比，Web 的图形化界面则要友好得多，操作起来自然也就更加简单方便。通过 Web 界面，可以对交换机的许多重要参数进行修改和设置，并可实时查看交换机的运行状态。

在利用 Web 浏览器访问交换机之前，应当确认已经做好以下准备工作。

(1) 在用于管理的计算机中安装 TCP/IP 协议，并且在管理用计算机和被管理的交换机上都已经配置好 IP 地址信息。

(2) 用于管理的计算机中安装有支持 Java 的 Web 浏览器，如 Internet Explorer 4.0 及以上版本、Netscape 4.0 及以上版本，以及 Oprea with Java。

(3) 在被管理的交换机上建立了拥有管理权限的用户账户和密码。

(4) 被管理交换机的 Cisco IOS 支持 HTTP 服务，并且已经启用了该服务。否则，应当通过 Console 端口升级 Cisco IOS 或启用 HTTP 服务。

在计算机上运行 Web 浏览器，并连接至被管理交换机的操作步骤如下。

(1) 运行支持 Java 的 Web 浏览器。

(2) 在地址栏中输入被管理交换机的 IP 地址(如 172.16.100.4)或为其指定的域名，然后按 Enter 键，显示图 6-22 所示的对话框。



图 6-22　用户确认

(3) 分别在“用户名”和“密码”文本框中，输入拥有管理权限的用户名和密码。用户名.密码应当事先通过 Console 端口进行设置。

(4) 单击“确定”按钮，建立与被管理交换机的连接，Web 浏览器中显示交换机的管理页面。图 6-23 所示的 Cisco Catalyst 3750-E 的 Web 管理界面。

(5) 通过 Web 界面查看交换机的各种参数和运行状态，并可根据需要对交换机的某些参数做必要的修改。

6.2.4 网管软件方式

使用网管软件对网络进行网络管理工作，可以使管理更加轻松，针对于不同的管理需求可以使用不同的网管软件，例如 Cisco 推出的管理 Cisco 交换机的 Cisco CNA(Cisco Network Assistant)，管理 Cisco 路由器的 Cisco SDM(Cisco Router and Security Device

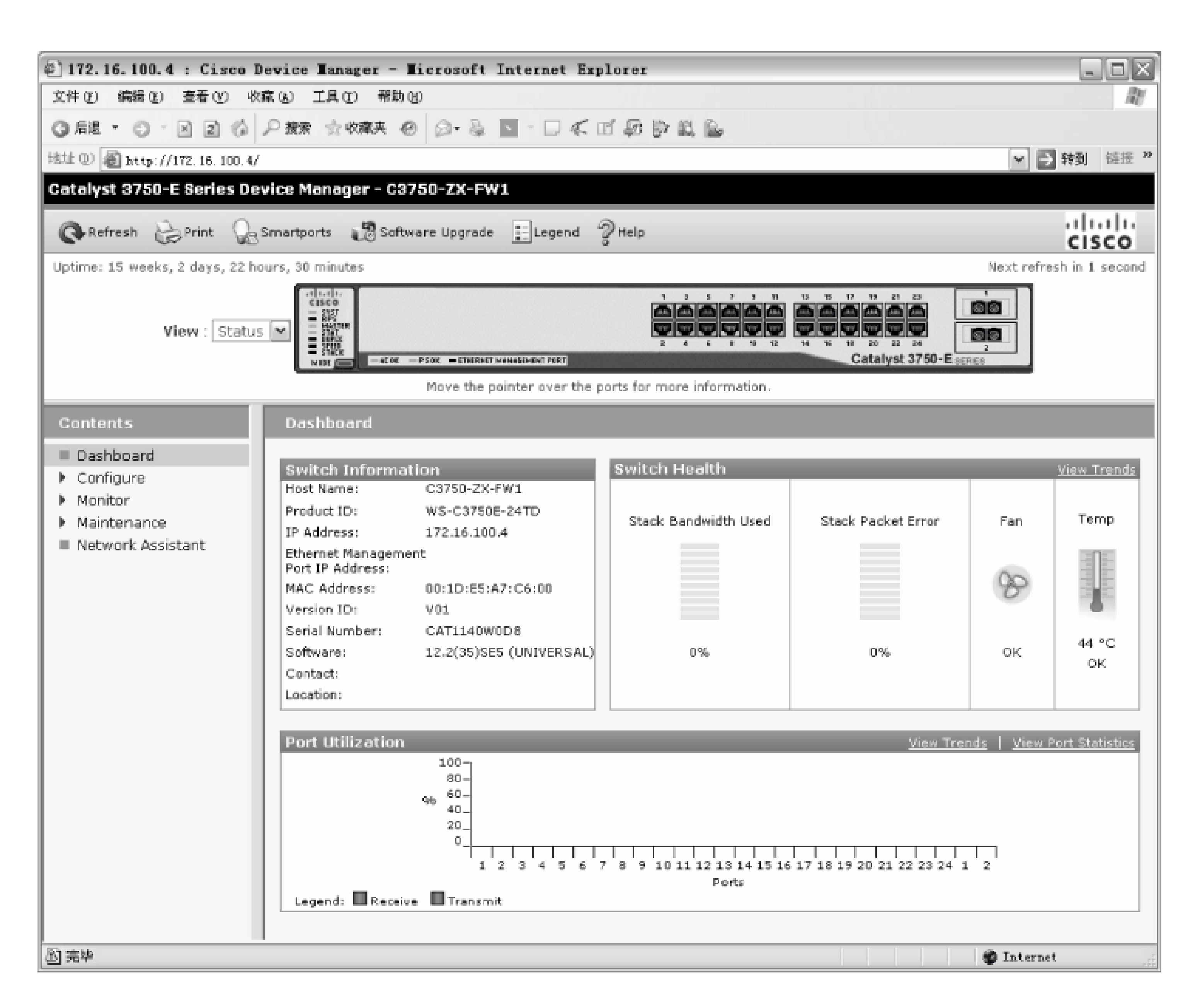


图 6-23　Web 管理界面

Manager)，以及用于管理 Cisco 自适应安全设备管理器的 ASDM(Adaptive Security Device Manager)等。另外，还可以使用一些综合性的网管软件对网络设备进行管理，例如 HP OpenView、CiscoWorks LMS 等。

6.3　网管前的准备

所有的网络设备在出厂前都进行了初始化配置，但仅使用这些配置是远远不能达到网络的使用要求的，且因为所有的设备的初始值相同或相似，将为日常管理中带来不便，所以，为了能够正常管理网络设备，需要根据管理要求对设备进行相应的配置。

6.3.1　交换机网管配置

在第一次配置交换机时，应当指定 IP 地址信息和名称，以便对该交换机进行远程管理。另外，还应当为交换机指定新的管理密码。交换机默认配置如表 6-1 所示。

表 6-1　交换机默认配置

特　征	默认配置	特　征	默认配置
IP 地址和子网掩码	无	Telnet 密码	无
默认网关	无	群集命令交换机	未启用
Enable Secret 密码	无	群集名称	无
主机名	Switch		

如果没有使用 Web 方式对交换机进行初始化，那么，仍然可以借助以下操作，通过 Console 端口实现对交换机的初始化配置。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 为交换机指定新的主机名,便于网络管理员标识和区分不同的交换机。

```
Switch(config)# hostname name
```

(3) 为特权模式指定新的密码。建议指定6位以上的密码,并同时包括大小写英文字母和数字。

```
Switch(config)# enable password password
```

(4) 进入Line配置模式,配置Telnet远程登录。

```
Switch(config)# line vty 0 15
```

(5) 为Telnet指定新的密码。

```
Switch(config-line)# password password
```

(6) 进入Line配置模式,配置Console端口。

```
Switch(config)# line console 0
```

(7) 为Console端口连接指定新的密码。

```
Switch(config-line)# password password
```

(8) 为该交换机指定默认网关。通常情况下,汇聚交换机和接入交换机的默认网关就是核心交换机的管理IP地址。

```
Switch(config)# ip default-gateway ip_address
```

(9) 进入VLAN 1。交换机的管理VLAN为VLAN 1,因此,为交换机指定IP地址信息时,必须进入VLAN 1中进行配置。

```
Switch(config)# interface vlan 1
```

(10) 为该交换机指定IP地址和子网掩码。

```
Switch(config-if)# ip address ip_address subnet_mask
```

(11) 激活并启用VLAN1。

```
Switch(config-if)# no shutdown
```

(12) 返回全局配置模式。

```
Switch(config-if)# exit
```

(13) 启用HTTP服务。

```
Switch(config)# ip http server
```

（14）返回特权配置模式。

```
Switch(config)# exit
```

（15）校验输入的信息是否正确。

```
Switch# show running-config
```

（16）保存配置。如果不保存，在交换机重新启动时，修改的配置将丢失。

```
Switch# copy running-config startup-config
```

6.3.2 路由器网管配置

路由器作为最重要的网络设备之一，其配置和管理是每个网络管理员所关注的。路由器的管理与一般计算机或者服务器的管理完全不同，路由器的管理和设置不当将直接影响到整个网络的正常运转，甚至还可能会埋下网络管理的安全隐患。不同品牌的路由器的配置方法也是不一样的，所以操作之前应该参照相应路由器配置手册。在将路由器添加至企业网络前，必须先对路由器做一些最基本的配置，以启用最基本的路由功能，并实现远程管理。

（1）当系统显示如下信息时，输入 no，将进入 CLI 配置模式。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

（2）按 Enter 键，停止自动配置，并开始手动配置。

```
Would you like to terminate autoinstall? [yes] Return
Several messages are displayed, ending with a line similar to the following:
...
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled date time by person
```

（3）按 Enter 键，显示 Router>提示符。

```
...
flashfs[4]: Initialization complete.Router>
```

（4）进入特权配置模式。

```
Router> enable
Router#
```

（5）进入 Enable 模式，当提示符改变为 Router# 时，输入口令。

```
Router>enable
Password: <password>
Router#
```

（6）进入全局配置模式，按 Ctrl+Z 键可退出该模式。

```
Router# configure terminal
Router(config)#
```

(7) 为该路由器设置一个有意义的名字,以取代默认的名称 Router。

```
Router(config)# hostname xxxx
xxxx(config)#
```

(8) 输入新的秘密口令 password,该口令用于进入特权命令模式。当用户在 Router>提示符下输入 enable 时,必须以该口令进行校验,以防止未经授权的用户修改路由器的设置。

```
Router(config)# enable secret password
```

(9) 进入 Line 配置模式,配置 Telnet 远程登录。

```
Switch(config)# line vty 0 15
```

(10) 为 Telnet 指定新的密码。

```
Switch(config-line)# password password
```

(11) 进入 Line 配置模式,配置 Console 端口。

```
Switch(config)# line console 0
```

(12) 为 Console 端口连接指定新的密码。

```
Switch(config-line)# password password
```

(13) 指定局域网接口,该接口直接连接到局域网。

```
Switch(config)# interface interface-id
```

(14) 指定局域网接口的 IP 地址和子网掩码。

```
Switch(config-if)# ip address ip_address subnet_mask
```

(15) 指定广域网接口,该接口连接到其他网络或 Internet。

```
Switch(config)# interface interface-id
```

(16) 指定广域网接口的 IP 地址和子网掩码。

```
Switch(config-if)# ip address ip_address subnet_mask
```

(17) 返回全局配置模式。

```
Switch(config-if)# exit
```

(18) 启用 HTTP 服务。

```
Switch(config)# ip http server
```

(19) 启用 IP 路由。

```
Switch(config)# ip route
```

(20) 将所有对外部的访问都路由至广域网或 Internet 接口。

```
Switch(config)# ip route 0.0.0.0 0.0.0.0 wan-interface-id
```

(21) 返回特权配置模式。

```
Switch(config)# exit
```

(22) 校验输入的信息是否正确。

```
Switch# show running-config
```

(23) 保存配置。如果不保存,路由器重新启动时,修改的配置将被丢失。

```
Switch# copy running-config startup-config
```

(24) 退出全局配置模式。

```
Router# exit
Router>
```

(25) 尝试以新口令重新进入。

```
Router> enable
Password: password
Router#
```

此时,即可借助 Telnet 等方式远程登录至该路由器进行管理。通常情况下,从内部网络访问路由器时,使用局域网接口的 IP 地址;从外部网络访问路由器时,使用广域网接口的 IP 地址。

6.3.3 安全设备网管配置

默认情况下,新购买的安全设备没有进行任何设置,如果欲使用 Cisco ASDM 管理安全设备,需要首先对安全设备进行初始化。

1. 开始前的准备

在开始运行 Startup Wizard(启动向导)之前,首先需执行下述操作。

(1) 获得一个 DES 许可证或 3DES-AES 许可证。

提示:运行 ASDM,必须拥有自适应安全设备的 DES 许可证或 3DES-AES 许可证。

(2) 在 Web 浏览器启用 Java and JavaScript。

(3) 搜集下列信息。

① 在网络中能够识别自适应安全设备的主机名。

② 外部接口、内部接口和其他接口的 IP 地址信息。

③ 用于 NAT 或 PAT 配置的 IP 地址信息。

④ DHCP 服务器的 IP 地址范围。

2. 使用 Startup Wizard

ASDM 使用 Startup Wizard 简单地初始化自适应安全设备。只需很少的几个步骤,启动向导就可以启用自适应安全设备,实现数据在内部接口(GigabitEthernet0/1)和外部接口(GigabitEthernet0/0)的安全传输。

(1) 如果是 ASA 5520 或 ASA 5540,使用跳线将入口 GigabitEthernet0/1 连接到交换机或其他集线设备。如果是 ASA 5510,使用跳线将入口 Ethernet 1 连接到交换机或其他

集线设备。然后，在同一台交换机上连接管理用计算机，实现对自适应安全设备的配置。

（2）配置计算机使用 DHCP 方式，将自动从自适应安全设备获得 IP 地址信息。需要注意的是，如果安全设备与计算机是通过交换机进行连接，在交换机所连接的网络中不应再包括其他 DHCP 服务器。

提示：这里将自适应安全设备的内部接口默认指定为 211.82.216.166。

（3）如果是 ASA 5520 或 ASA 5540，检查 GigabitEthernet0/1 接口的 LINK LED 指示灯。如果是 ASA 5510，则检查 Ethernet 1 接口的 LINK LED 指示灯。当连接正常时，相应接口的 LINK LED 指示灯应当呈绿色。

（4）运行 Startup Wizard 启动向导。在配置计算机上运行 Web 浏览器，在“地址”栏中输入 https:// 211.82.216.166/，并按 Enter 键。

（5）单击 Run ASDM 按钮，显示图 6-24 所示的 Cisco ASDM Launcher 窗口。根据需要分别输入安装设备的 IP 地址、用户名和密码，默认情况下密码为空。

（6）单击 OK 按钮，显示图 6-25 所示的“警告-安全性”对话框，提示需要安装数字证书。



图 6-24　Cisco ASDM Launcher 窗口

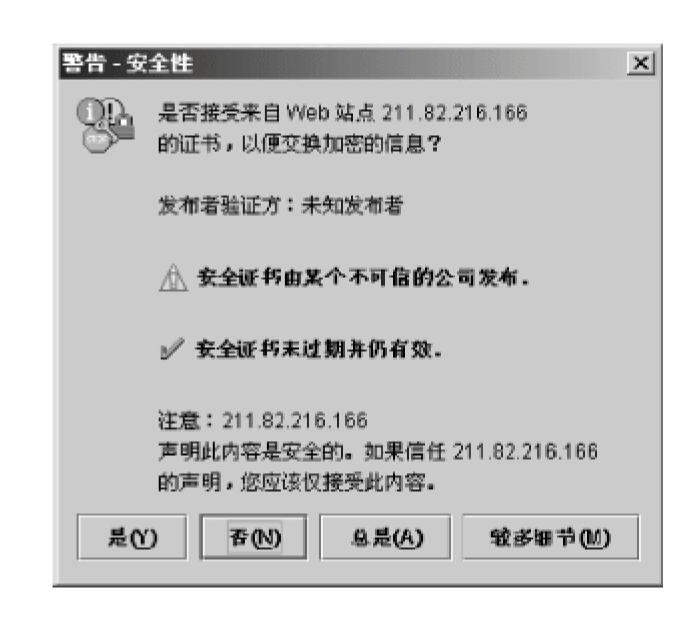


图 6-25　“警告-安全性”对话框

（7）单击“是”按钮，ASDM 即可启动。

（8）依次选择 Wizards→Startup Wizard 命令，运行安装向导。根据启动向导中的提示，设置自适应安全设备。

6.3.4　无线设备网管配置

使用无线局域网控制器附带的 Console 线，将计算机的串行端口连接至无线局域网控制器的 Console 端口，启用超级终端建立彼此之间的连接。

（1）将控制器连接至电源，打开控制器背板上的电源开关。

（2）使用 CLI 界面观察引导过程。引导脚本显示操作系统软件初始化和基本配置，大致内容如下。

```
Bootloader 3.4.0.0. (Jun 2 2008-15:07:12)
Motorola PowerPC ProcessorID=00000000 Rev. PVR=80200020
Cisco Systems INC., 4400 Wireless LAN Switch Board
    CPU: 833 MHz
    CCB: 333 MHz
    DDR: 166 MHz
    LBC: 41 MHz
...
```

```
Device 1: not available
Booting Primary Image...
Press <ESC> now for additional boot options...
```

(3) 如果需要，按 Esc 键显示引导选项菜单。

```
Boot Options
Please choose an option from below:
1. Run primary image
2. Run backup image
3. Manually update images
4. Change active boot image
5. Clear Configuration
Please enter your choice:
```

输入“1”运行当前的软件映像，输入“2”运行较早前的软件映像，输入“5”运行当前的软件映像并将控制器配置恢复至出厂默认状态。在没有专家指导的情况下，不推荐输入“3”或“4”。

```
Detecting Hardware ...
```

(4) 整个引导过程大致持续 2～3 分钟，在用户登录提示符出现之间，请勿重新引导控制器。

```
Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.

Cisco AireOS Version 3.4.0.0
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
...
Starting Management Services:
    Web Server: ok
    CLI: ok
    Secure Web: ok
```

(5) 如果控制器完成加电自检，引导脚本运行开始向导，提示用户进行控制器的基本配置。为控制器输入系统名称，最多 32 个 ASCII 字符。

(6) 如果想要使控制器的服务端口从 DHCP 服务器获得 IP 地址，输入 dhcp。如果不想使用服务端口，或者想为服务端口指定 IP 地址时，输入 none。

注意：服务端口的 IP 地址必须与和 AP-manager 接口位于不同的子网。

(7) 如果在第 6 步中输入 none，输入服务端口的 IP 地址和子网掩码。为管理端口输入 IP 地址、子网掩码和网关 IP 地址，并选择 VLAN ID。

注意：VLAN ID 的设置应当与交换机接口配置相匹配。

(8) 输入用于为无线客户端分配 IP 地址的 DHCP 服务器的 IP 地址，控制器管理接口的 IP 地址，以及服务端口的 IP 地址(可选)。

(9) 输入控制器 AP-manager 接口的 IP 地址。

AP-manager 接口使用三层安全机制在控制器和轻型无线 AP 之间通信。必须使用独一无二的 IP 地址，并且通常与管理接口配置相同的 VLAN 或子网，但是，该配置并非必需。如果 AP-manager 接口与管理接口位于相同的子网，两者将使用同一 DHCP 服务器的 IP 地址。

(10) 输入控制器虚拟接口的 IP 地址，将被用于所有控制器三层安全和移动管理。应使用一个没有被指定过的 IP 地址，如 1.1.1.1。

注意：虚拟接口用于支持移动管理、DHCP 中继和嵌入式三层安全。处于同一移动组的所有控制器都必须为虚拟接口配置相同的 IP 地址。

(11) 如果需要，输入控制器欲归属其中的移动组/RF 组的名称。

(12) 输入网络名称或 SSID(Service Set Identifier)。

(13) 输入 yes 允许客户端指定自己的 IP 地址。输入 no 则客户端向 DHCP 服务器请求分配 IP 地址。

(14) 配置 RADIUS 服务器。输入 Yes，并指定 RADIUS 服务器 IP 地址、通信端口和机密密钥。输入 no，不指定 RADIUS 服务器。

(15) 输入国家代码。输入 help，可显示国家代码列表。

(16) 输入 Yes，启用 RRM 自动 RF 功能。输入 no，则禁用该功能。

(17) 控制器保存配置、重新引导后，提示用户重新登录。输入有效的用户名和密码，登录控制器 CLI 界面。显示如下提示符。

```
#(system prompt)>
```

6.4　配置和映像文件的备份与恢复

TFTP(Trivial File Transfer Protocol)服务器可实现交换机或交换机软件系统的保存和升级、配置文件的保存和下载，使得对交换机和交换机的管理变得简单和快捷。因此，在进行交换机和交换机的管理前，应先安装一台 Cisco TFTP 服务器。TFTP 服务器软件可在 Cisco 网站(http://www.cisco.com/)下载。任何一台计算机只要安装有 TFTP 服务器软件，即可成为 TFTP 服务器。

6.4.1　配置文件的备份与恢复

网络设备的系统文件和配置文件都可以像计算机之间复制文件一样互相复制。无论是上传还是下载文件，都必须在操作终端上安装 TFTP 软件，将其配置成为 TFTP 服务器。

1. 将配置文件备份至 TFTP

利用上传的配置文件，不仅可以快速恢复原有交换机的配置，而且还可用于快速配置其他交换机，减少配置的劳动强度，提高工作效率。

在将配置文件上传至 TFTP 服务器之前，确认已经完成以下工作。

(1) 确认已经安装了一台 TFTP 服务器。

(2) 确认交换机能够与 TFTP 服务器正常通信，交换机和路由器必须位于同一子网。

(3) 在上传映像之前，可能需要在 TFTP 服务器上创建一个空的文件。

(4) 如果覆盖一个已经存在的文件(包括空文件，如果已经创建)，确认赋予了相应的权

限，即赋予其 world-write 权限。

然后，将配置文件上传至 TFTP。

（1）通过 Console 端口或 Telnet 登录至交换机，如图 6-26 所示。

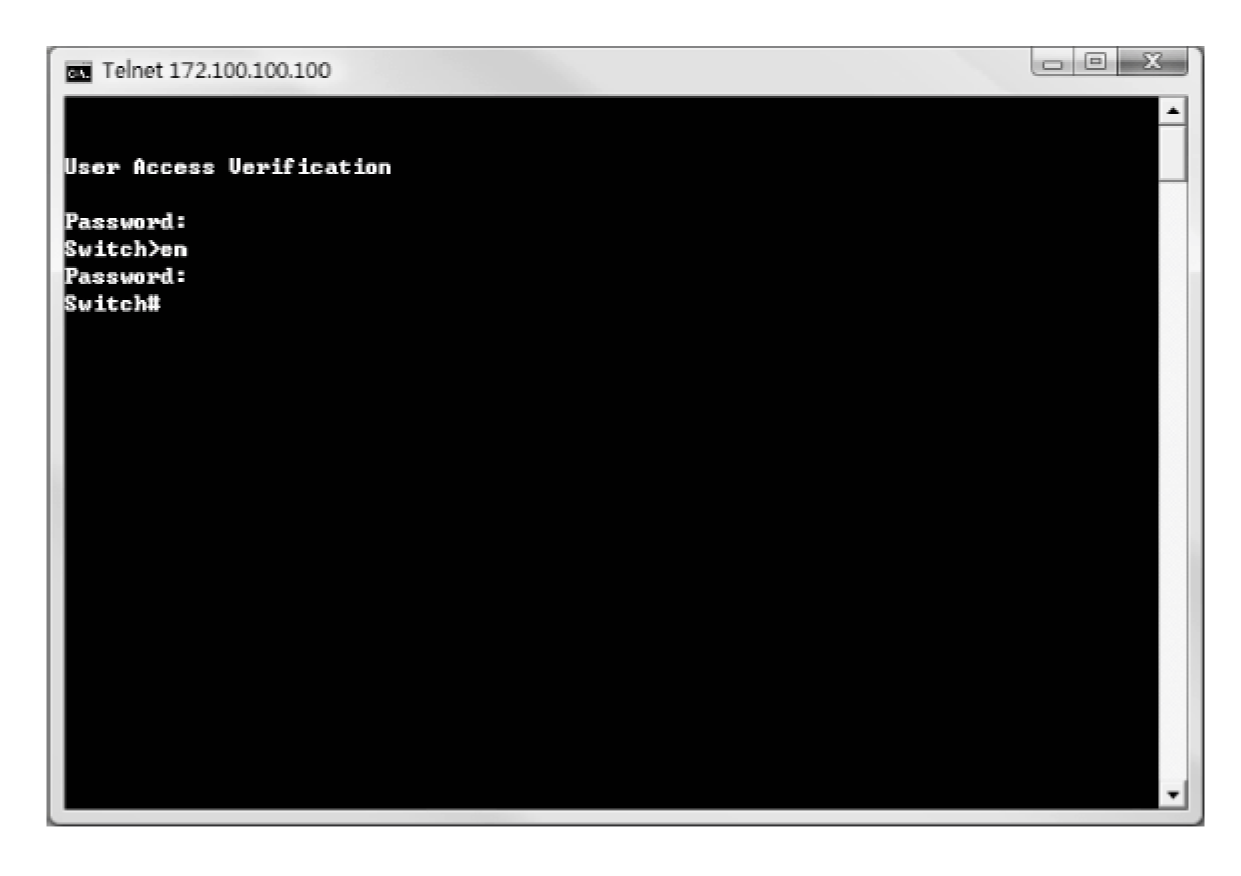


图 6-26　登录交换机

（2）运行 copy running-config tftp 命令，将配置文件上传至 TFTP 服务器。在提示符下，指定 TFTP 服务器的 IP 地址或主机名，以及目的文件名，如图 6-27 所示。配置文件将被上传至 TFTP 服务器。

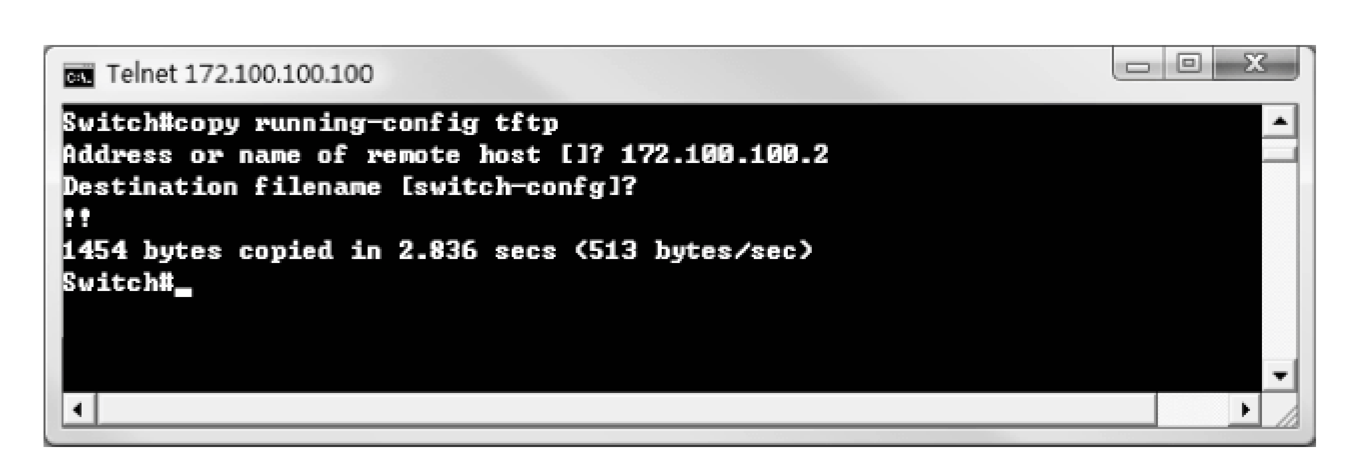


图 6-27　上传配置文件

在 Cisco TFTP Server 窗口，即可显示上传的具体信息，如图 6-28 所示。

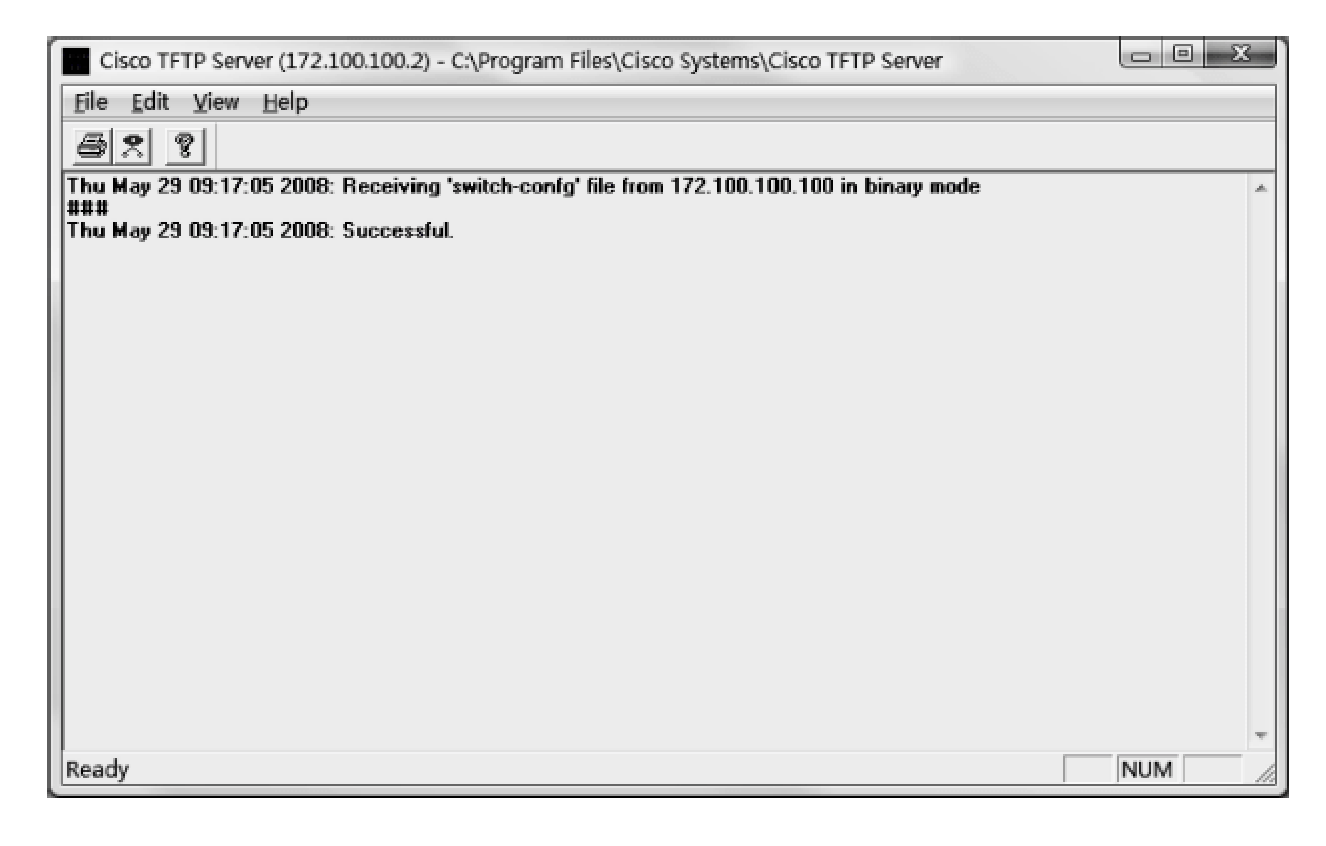


图 6-28　Cisco TFTP Server 窗口

2. 从 TFTP 恢复配置文件

在从 TFTP 服务器下载配置文件前，确认已经完成以下工作。

(1) 确认已经安装了一台 TFTP 服务器。

(2) 确认交换机能够与 TFTP 服务器正常通信，交换机和路由器必须位于同一子网。

(3) 确认配置文件被下载至服务器的适当目录。

(4) 确认文件被设置了 world-read 权限。

然后，从 TFTP 服务器下载配置文件。

(1) 将配置文件复制至 TFTP 服务器的适当目录。

(2) 通过 Console 端口或 Telnet 登录至交换机。

(3) 运行 copy tftp running-config 命令，利用从 TFTP 服务器下载的配置文件配置交换机。指定 TFTP 服务器的 IP 地址或主机名，以及下载文件的文件名。配置文件被下载。

6.4.2 映像文件的备份与恢复

映像文件是指网络设备的系统文件，即通常所说的 IOS。映像文件是网络设备正常启动的保证。如果网络设备没有映像文件则不能启动。

1. 备份系统软件映像

在将软件映像上传至 TFTP 服务器之前，确认已经完成以下工作。

(1) 确认已经安装了一台 TFTP 服务器。

(2) 确认交换机能够与 TFTP 服务器正常通信，交换机和路由器必须位于同一子网。

(3) 在上传映像之前，可能需要在 TFTP 服务器上创建一个空的文件。

(4) 如果覆盖一个已经存在的文件(包括空文件，如果已经创建)，确认赋予了相应的权限，即赋予其 world-write 权限。

然后，使用 TFTP 服务器上传软件映像。

(1) 通过 Console 端口或 Telnet 登录至交换机。

(2) 使用 copy flash tftp 命令，将软件映像上传至 TFTP 服务器。在提示符下，指定 TFTP 服务器地址和目的文件名。系统映像将被上传至 TFTP 服务器。

2. 恢复或升级系统软件映像

使用 TFTP 服务器，可以通过网络将系统软件映像文件下载到交换机，该映像文件将会被下载至超级引擎的 Flash 内存中。在 Flash 内存中可以保存多个映像文件。

在使用 TFTP 下载软件系统映像前，确认已经完成下述工作。

(1) 确认已经安装了一台 TFTP 服务器。

(2) 确认交换机能够与 TFTP 服务器正常通信，交换机和路由器必须位于同一子网。

(3) 确认软件映像被下载至 TFTP 服务器适当的目录中。

(4) 确认文件的访问许可设置正确。

(5) 确认提供了不间断电源。

然后，使用 TFTP 下载超级引擎映像。

(1) 将软件映像复制至 TFTP 服务器适当的目录。

(2) 通过 Console 端口或 Telnet 登录至交换机。如果使用 Telnet 登录交换机，那么，

当交换机运行新软件而重新启动时，将断开连接。

(3) 使用 copy tftp flash 命令从 TFTP 服务器下载软件映像。在提示符下输入 TFTP 服务器的 IP 地址或主机名，以及下载的文件名。交换机将从 TFTP 服务器下载映像文件，并将映像复制至引导闪存。

(4) 使用 set boot system flash device:filename prepend 命令修改 BOOT 变量值，当交换机重新启动时，使用新的映像引导。指定 Flash 设备(Device)和下载的映像文件名(Filename)。

(5) 使用 reset system 命令重新启动交换机。如果使用 Telnet 连接至交换机，那么，该 Telnet 进程将断开连接。

(6) 当交换机重新引导后，输入 show version 命令检查交换机上的编码版本。

6.4.3 映像文件的版本与选择

Cisco IOS 是思科公司的网络操作系统，是一个为网际互联优化的复杂的操作系统，其性质类似于局域操作系统(NOS)，如 Novell 的 NetWare。IOS 是一个与硬件分离的软件体系结构，随着网络技术的不断发展，可动态升级以适应不断变化的技术。在实际使用中，需要根据需要选择所使用的 IOS 版本。实际上，Cisco 已经提供了一种用于 Cisco IOS 版本选择的工具，使用该工具可以根据需要选择所要使用的功能，并选择 Cisco IOS 版本。需要注意的是，在使用该工具前，首先需要在思科的官方网站(www.cisco.com.cn)注册 CCO 账号。

1. 选择 IOS 版本标准

思科公司提供 4 种选择 IOS 版本的方式，具体内容如下。

(1) 根据设备型号选择：不同的设备会因为硬盘配置等原因，适用的 IOS 版本也有所不同，例如在选择 IOS 版本时，需要考虑设备的 Flash 容量、内存大小等。

(2) 根据技术选择：使用该标准进行搜索，可以选择支持特定技术的 Cisco IOS。

(3) 根据功能选择：不同的 IOS 所包含的功能是不相同的。通常情况下，为了保证设备的运行状态，建议不选择包含不使用的功能的 IOS 版本。

(4) 根据版本选择：除以上标准外，还可以直接根据 Cisco IOS 的版本进行选择，并查看是否支持指定的设备。

2. 选择 IOS 版本

(1) 根据设备型号选择

根据设备型号选择 IOS 版本的步骤如下。

① 打开 IE 浏览器，在地址栏中输入如下内容：http://tools.cisco.com/ITDIT/ISTMAIN/servlet/index，显示图 6-29 所示的“连接到 tools.cisco.com”对话框，分别在“用户名”和“密码”文本框中输入申请的 CCO 账号和密码。



图 6-29 “连接到 tools.cisco.com”对话框

② 单击“确定”按钮，显示图 6-30 所示的 Cisco IOS Software Selector 窗口。

③ 单击 Search by Product 链接，显示图 6-31 所示的 Search by Product 窗口。

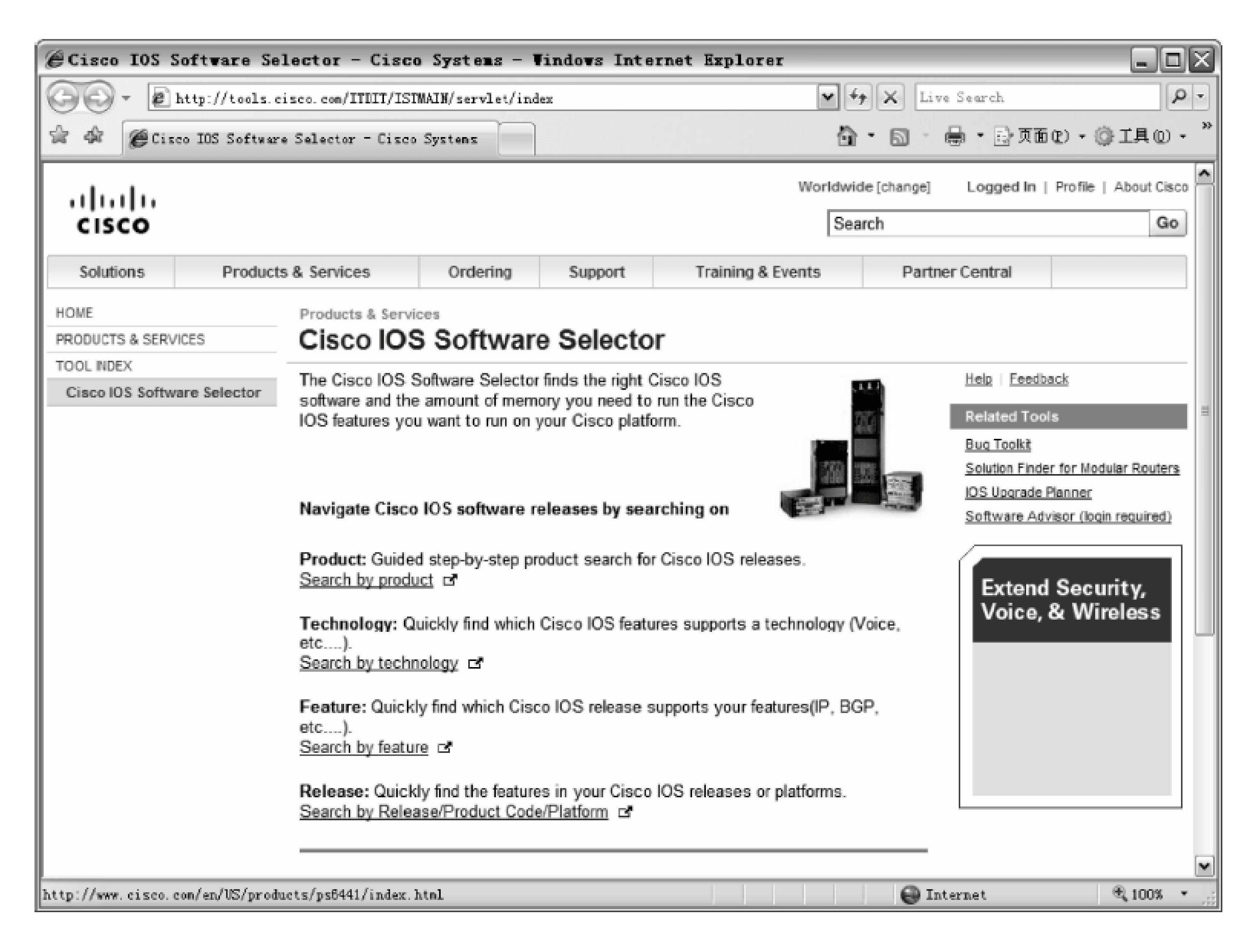


图 6-30　Cisco IOS Software Selector 窗口

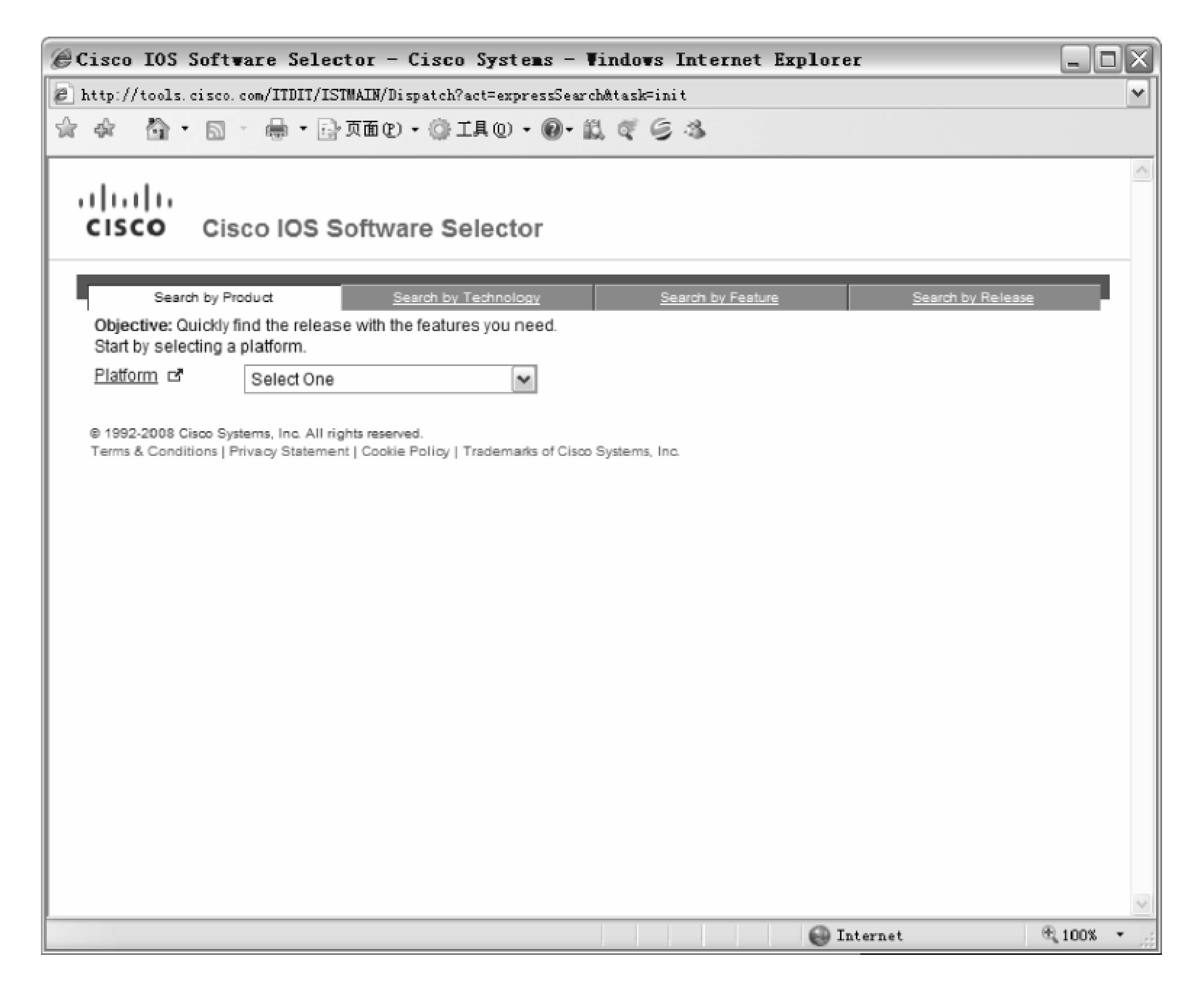


图 6-31　Search by Product 窗口

④ 在 Platform 下拉列表框中，选择设备型号，例如这里选择 2811。在 Search by full or partial feature name 文本框中，输入具有全部或部分功能的名称，如图 6-32 所示。

⑤ 单击 Search 按钮，显示图 6-33 所示的 Results 列表。在 Features avaliable 列表中，显示可用的功能列表。选择所需的功能，单击 Add 按钮，将其添加到右侧列表中即可。

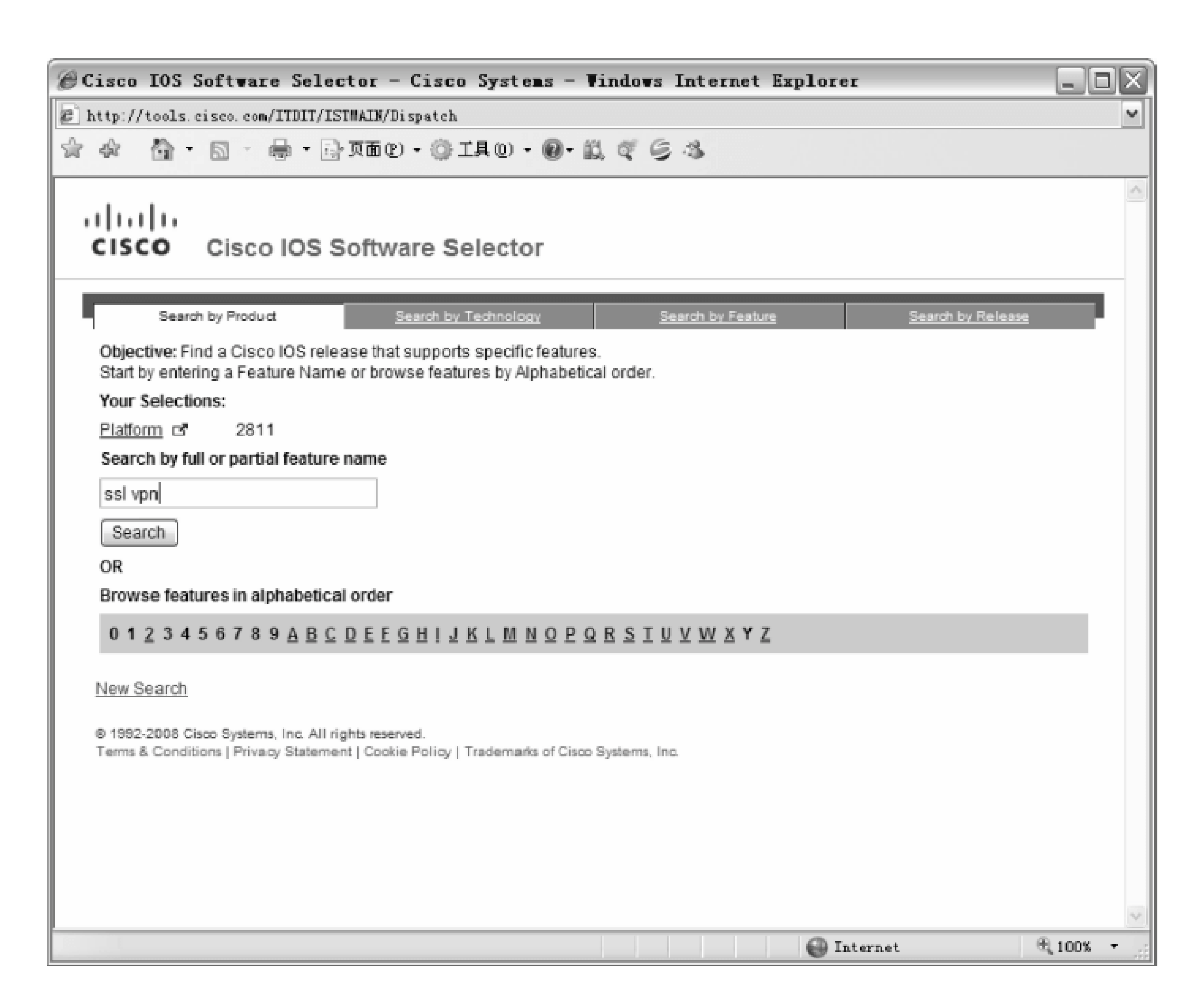


图 6-32 搜索具有全部或部分功能的版本

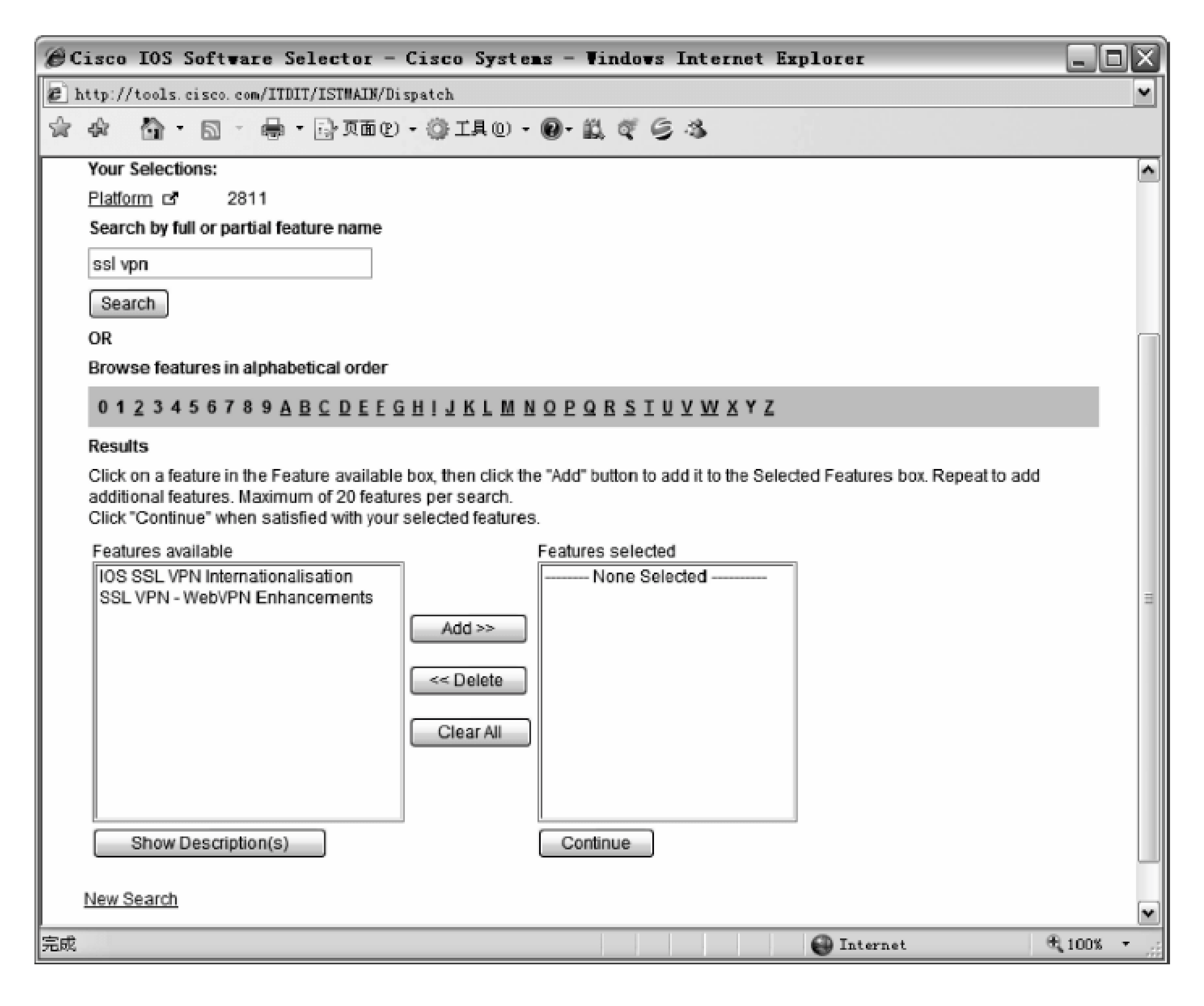


图 6-33 Results 列表

⑥ 单击 Continue 按钮，显示图 6-34 所示的 Select a Major Cisco IOS Release 窗口。

⑦ 在 Cisco IOS Major Release 下拉列表框中，选择一个主要的 IOS 版本，例如这里选择 12.4T 版本，如图 6-35 所示。

⑧ 在 Release 下拉列表框中，选择一个 IOS 的子版本，例如这里选择 12.4(22)T，如图 6-36 所示。在 Feature Set 下拉列表框中，选择所需的功能。此时，在下方即可显示搜索

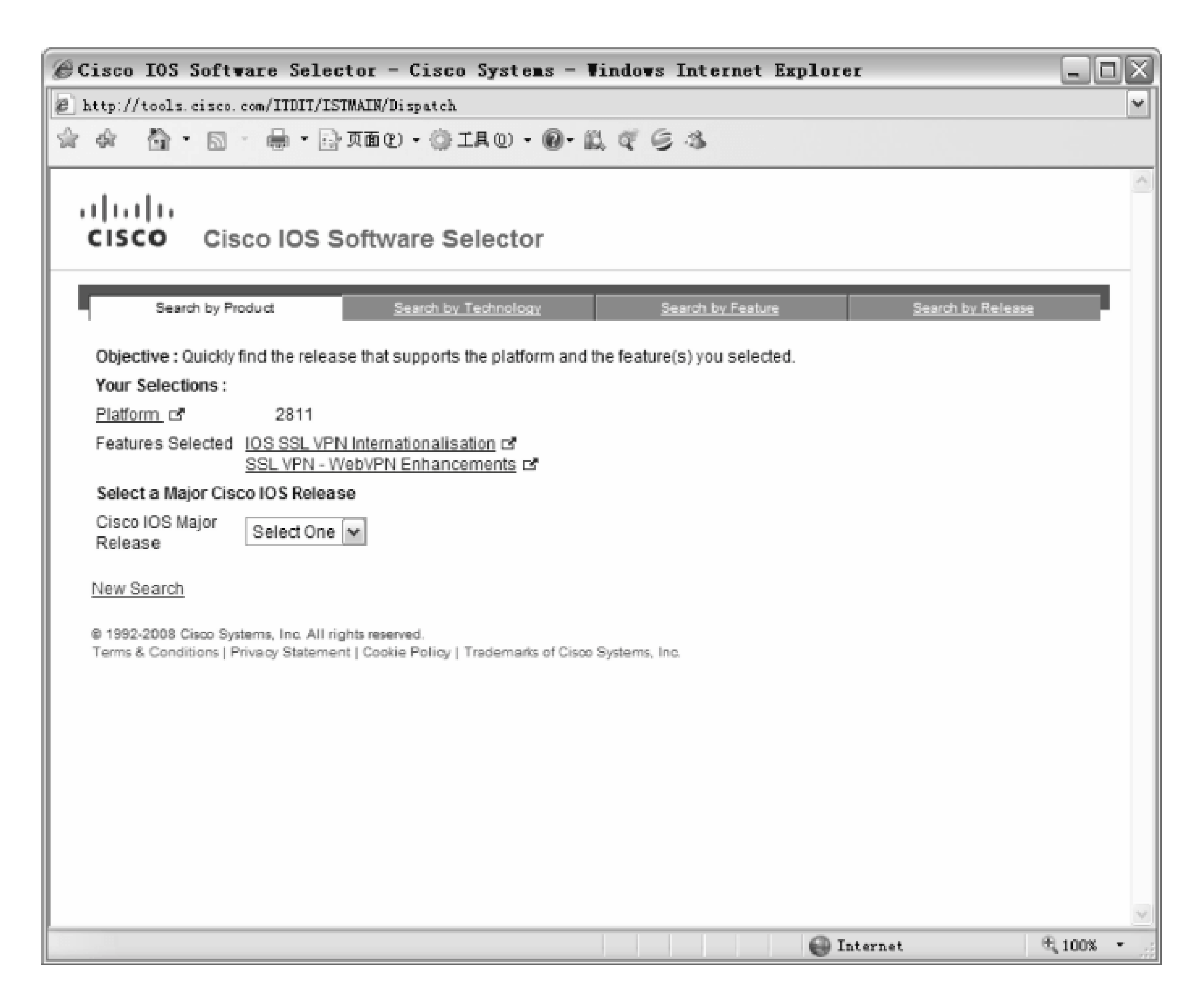


图 6-34　Select a Major Cisco IOS Release 窗口

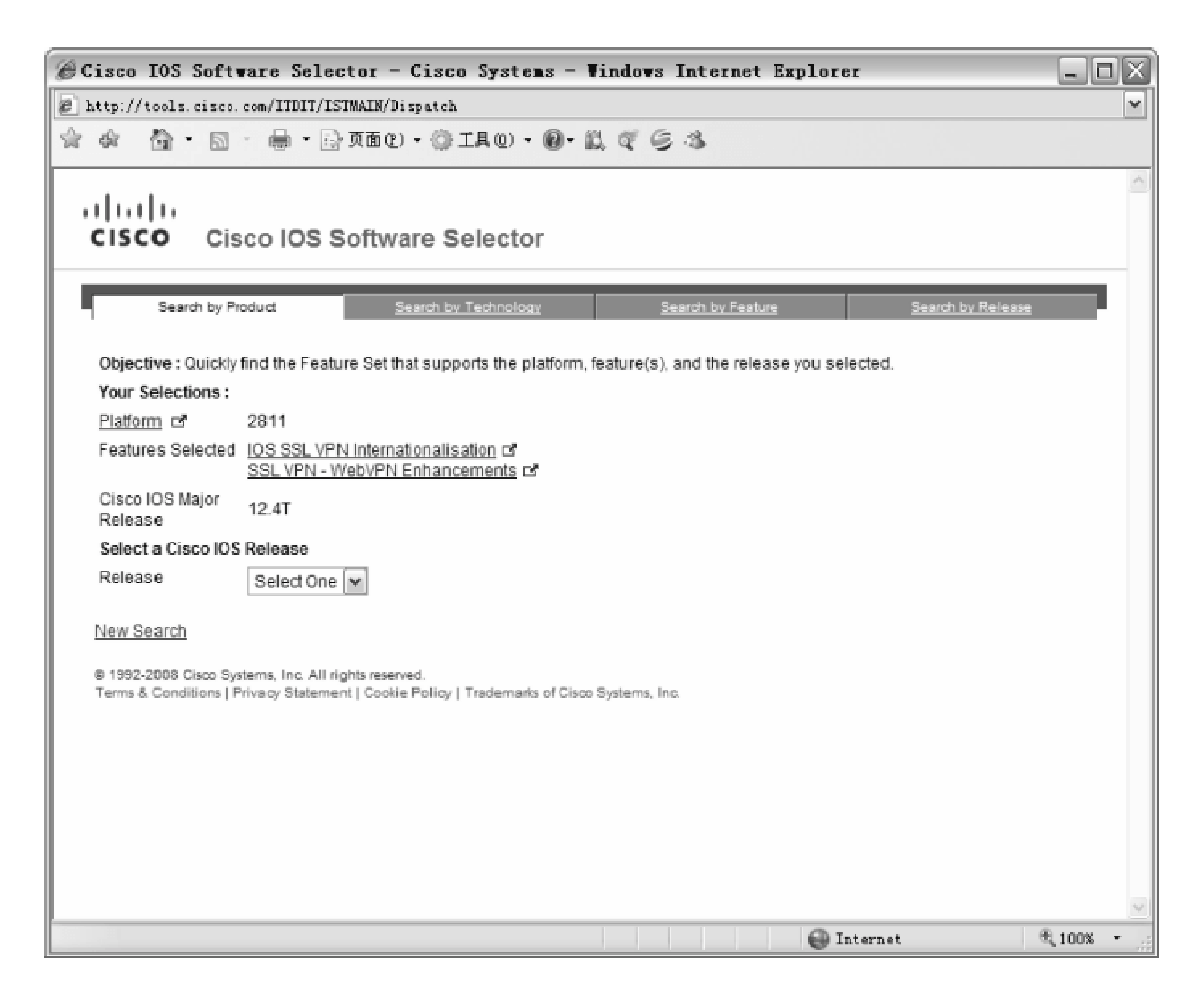


图 6-35　选择 IOS 主要版本

结果，在 Image Info 栏中，显示搜索到的 IOS 名称和产品号码等信息。在 Features 栏中，显示该版本的 IOS 所包含的功能。

（2）根据技术选择

根据技术选择 IOS 版本的步骤如下。

① 在 Cisco IOS Software Selector 窗口中，选择 Search by Technology 链接，或在 Search by Product 页面中，选择 Search by Technology 选项卡，如图 6-37 所示。

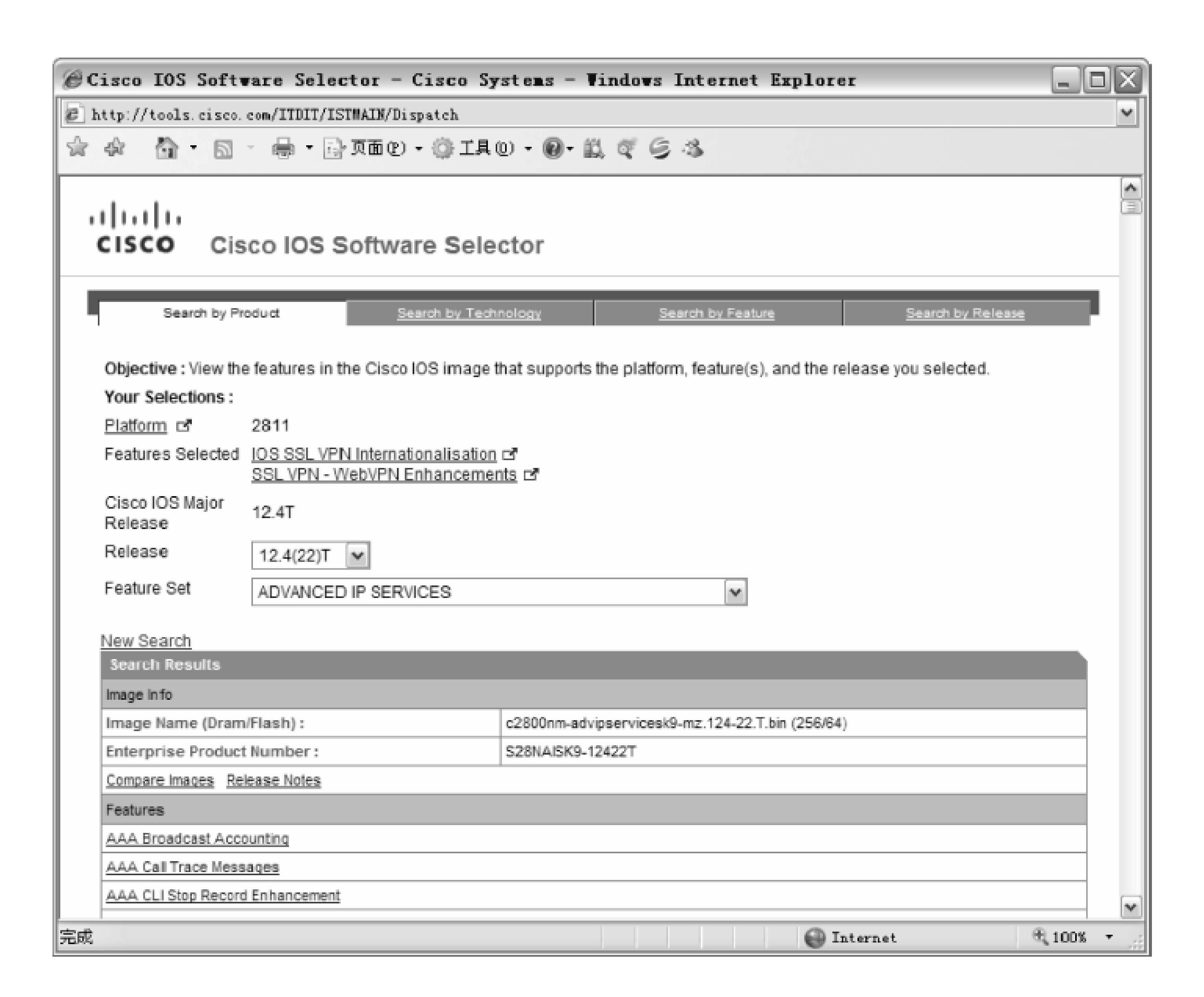


图 6-36　搜索结果

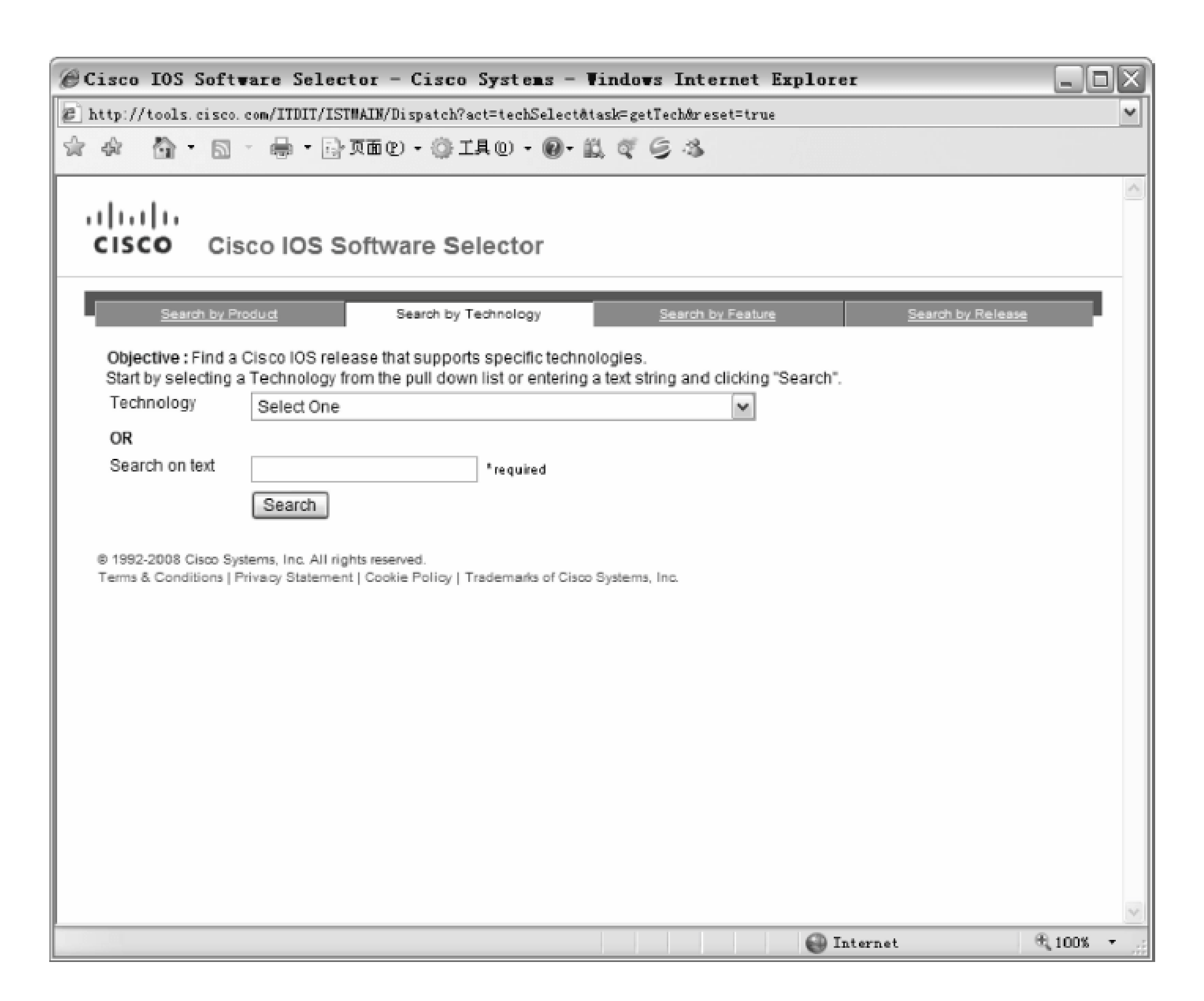


图 6-37　Search by Technology 窗口

② 在 Technology 下拉列表框中，选择所要使用的技术名称，例如这里选择 Security and VPN 选项。在 Sub Technology 下拉列表框中，选择所选技术的子技术。在下面的列表中，选中所要使用技术前的复选框，如图 6-38 所示。

③ 单击 Submit 按钮，显示图 6-39 所示的 Results 窗口。在 Selected Features 列表中，确认所选的技术。

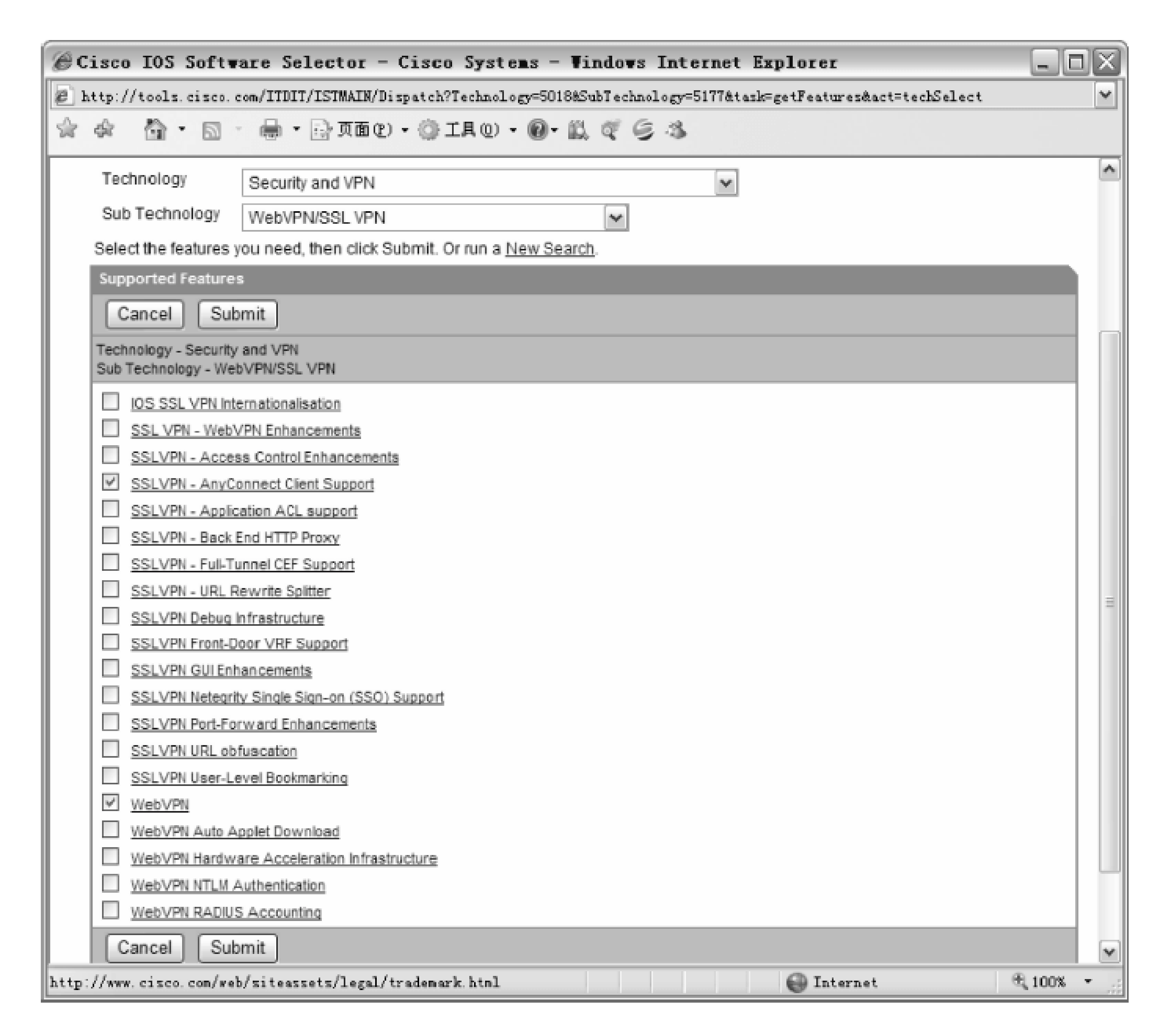


图 6-38　选择所要使用的技术

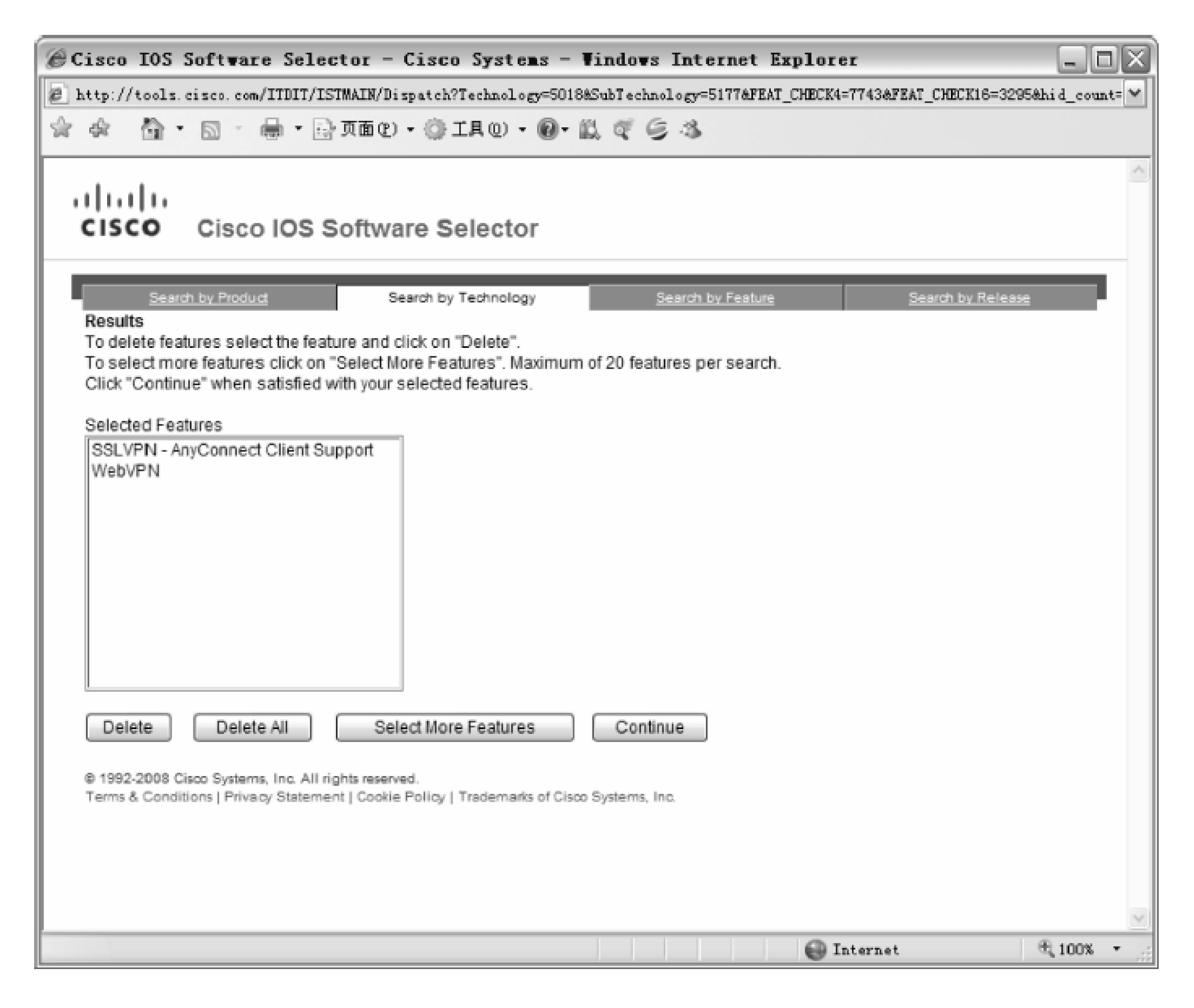


图 6-39　Results 窗口

④ 单击 Continue 按钮，显示图 6-40 所示的页面。根据需要选择 IOS 的版本内容，其设置方法同根据设备型号选择相同，这里就不再赘述。

（3）根据功能选择

根据功能选择 IOS 版本的步骤如下。

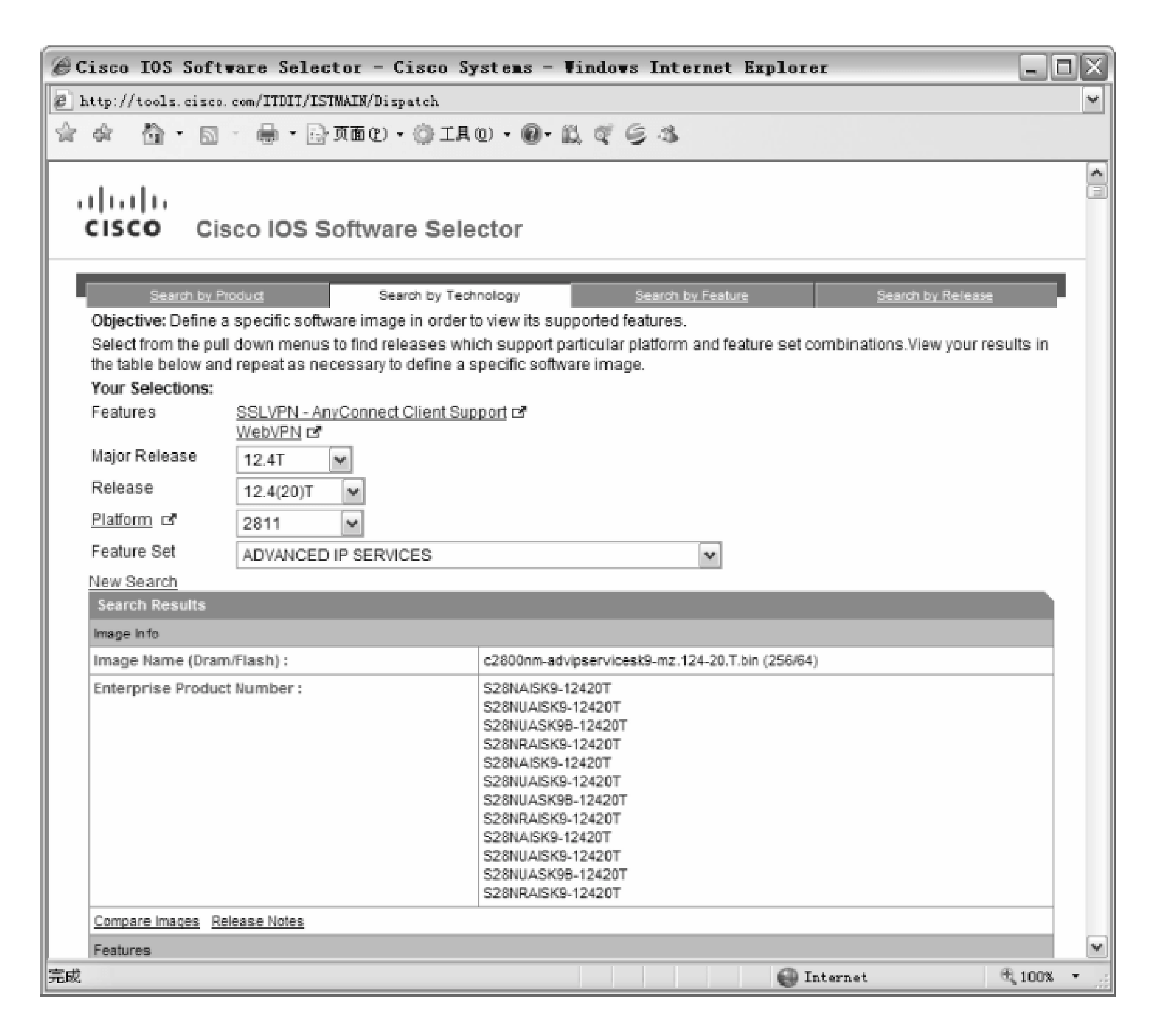


图 6-40　搜索结果

① 在 Cisco IOS Software Selector 窗口中，选择 Search by Feature 链接，或在 IOS 软件选项页面中，选择 Search by Feature 选项卡，如图 6-41 所示。在 Search by full or partial feature name 文本框中，输入所要使用的一个或多个功能。

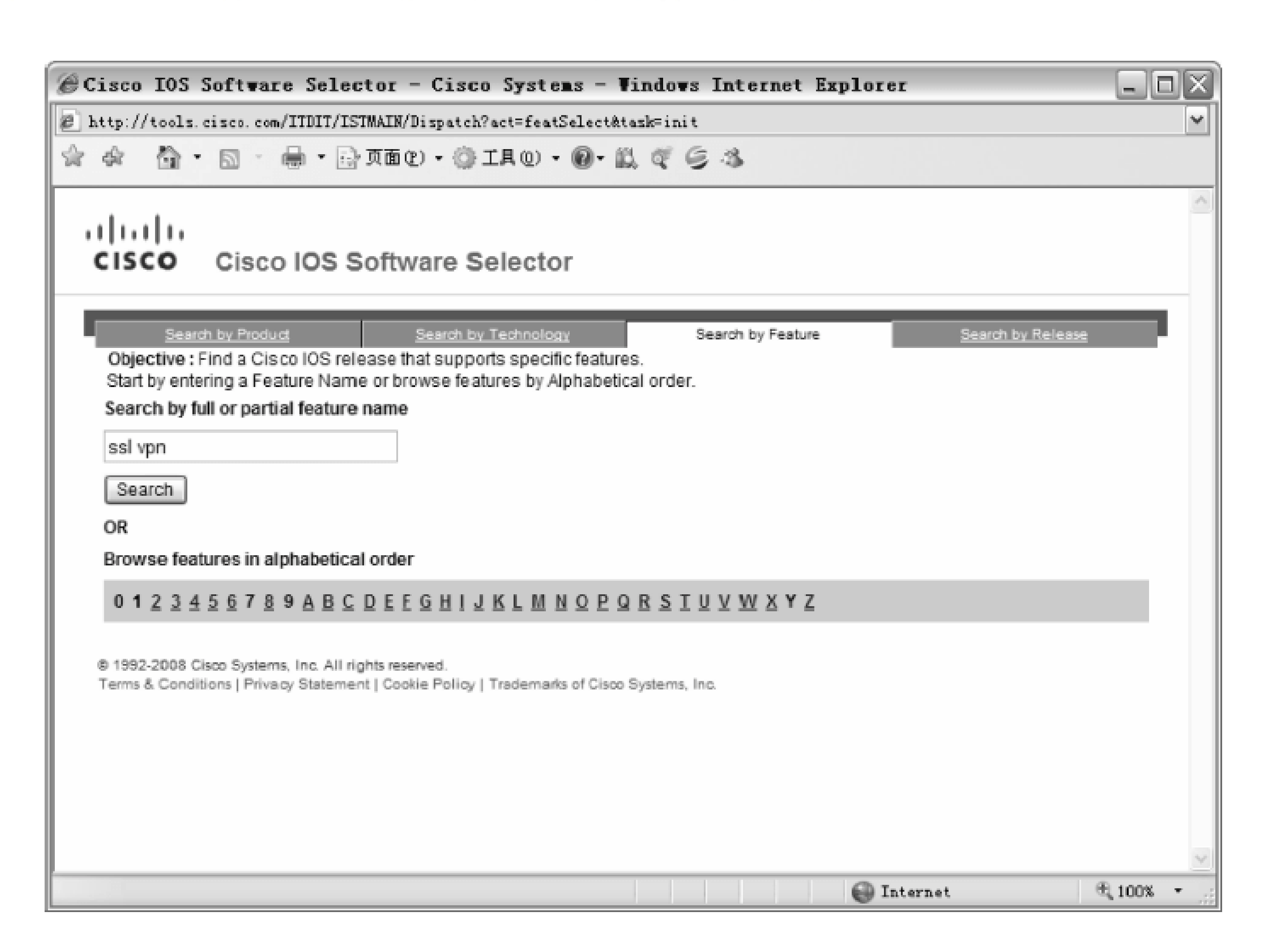


图 6-41　Search by Feature 窗口

② 单击 Search 按钮，显示图 6-42 所示的页面。在 Features avaliable 列表中，显示可用的功能列表。选择所需的功能，单击 Add 按钮，将其添加到右侧列表中即可。具体操作与根据设备型号选择相同，这里就不再赘述。

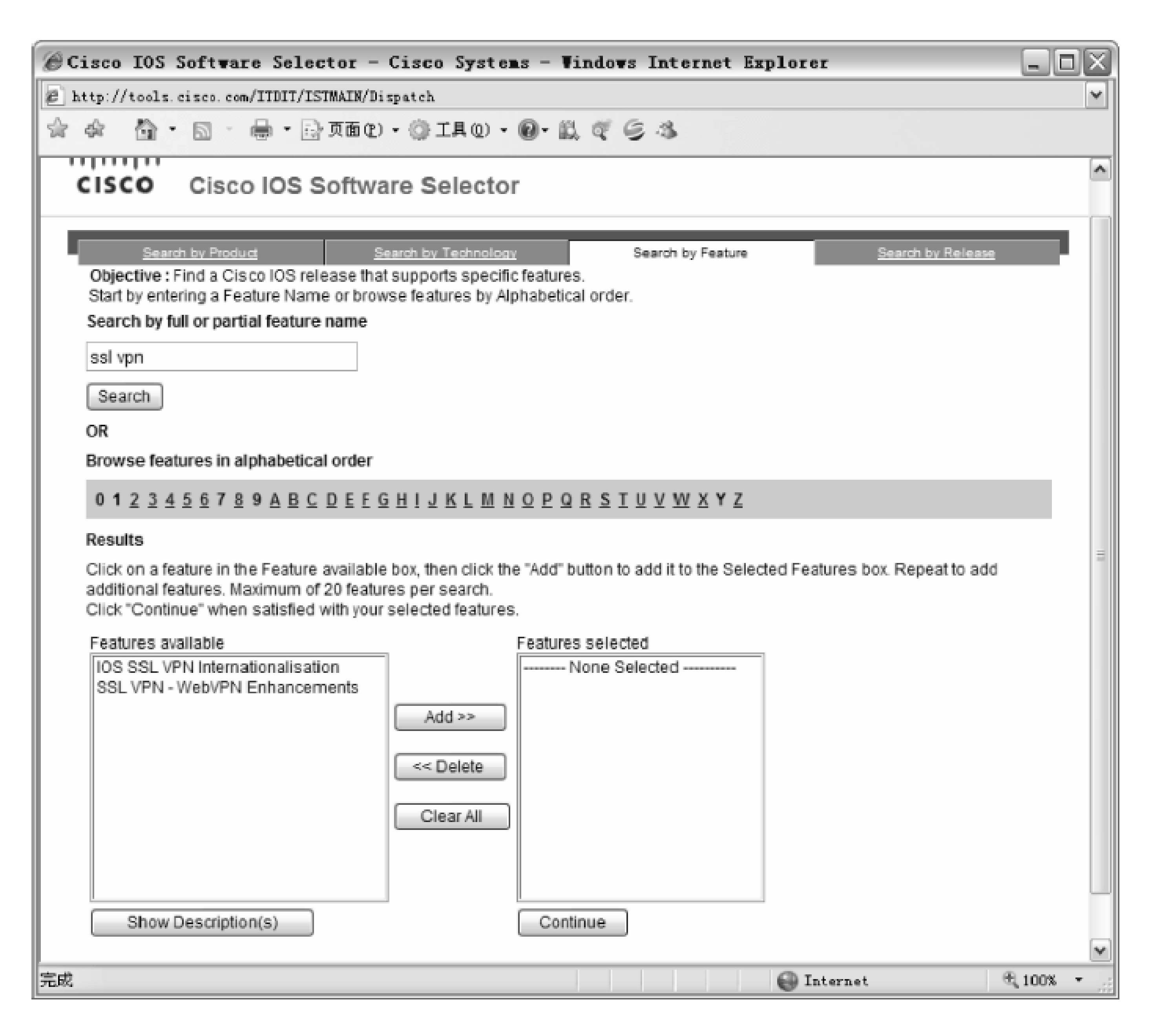


图 6-42　选择功能

(4) 根据版本选择

根据版本选择 IOS 版本的步骤如下。

① 选择图 6-43 所示的 Search by Release 选项卡，显示了 Cisco 所有的 IOS 版本信息。也可以在下方选项区域中，根据实际需要进行搜索，包括 IOS 主要版本、设备类型和设备号

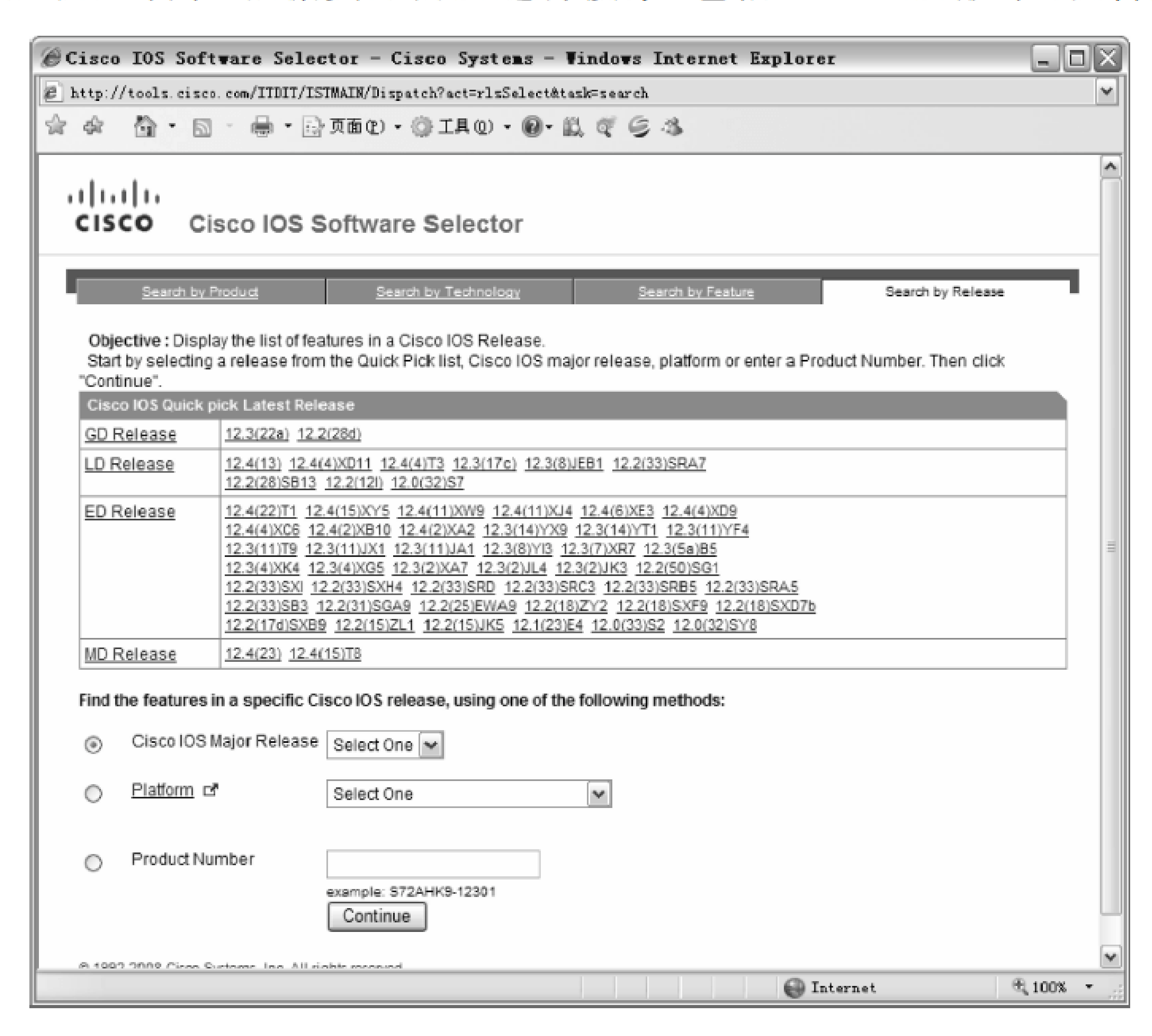


图 6-43　Search by Release 窗口

码。这里选中 Platform 单选按钮，根据设备类型选择 IOS 版本。在下拉列表框中选择 7200 选项，选择 7200 系列设备的 IOS。

② 单击 Continue 按钮，显示图 6-44 所示的窗口。具体各选项设置方法同根据设备型号选择相同，这里不再赘述。

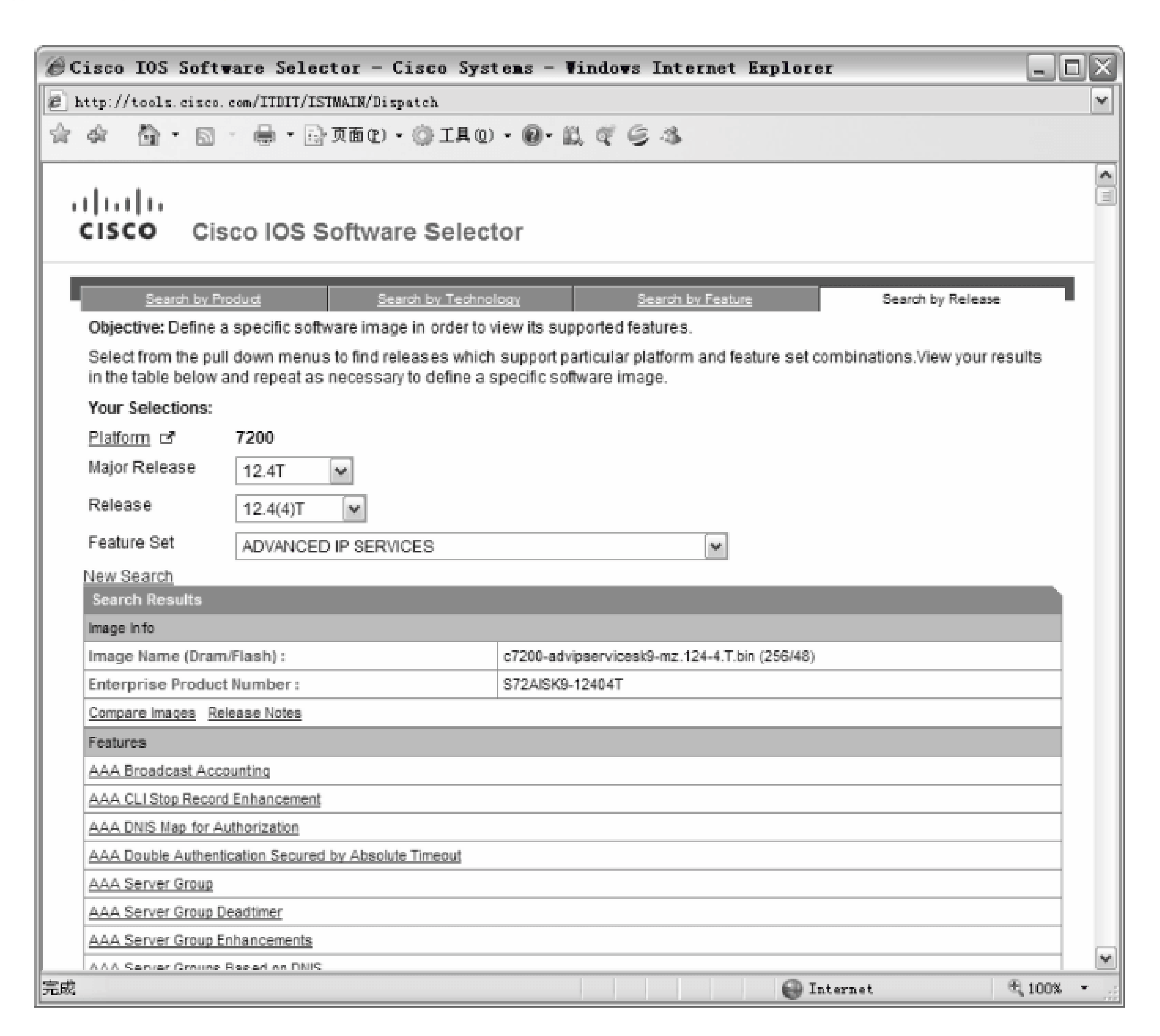


图 6-44 根据设备类型选择 IOS 版本

6.5 密码恢复

由于种种原因（如工作移交、技术文档丢失），网络管理员可能会遗失网络设备的密码。而丢失密码将意味着无法实现对网络设备的管理。事实上，只需通过简单的几个步骤，即可清除原来设置的密码，并重新设置新的密码。当然，为了访问安全起见，密码的清除工作必须通过 Console 端口才能完成。

6.5.1 交换机密码恢复

在实际工作中，很有可能遇到忘记控制台口令的事情。但没有口令就不能进入特权用户级，也就不能对路由器做配置。此时，则需要对设备的密码进行恢复操作，即恢复密码的出厂设置。

（1）拔掉网络设备的电源线。

（2）利用 Console 线将计算机的串行口与路由器的 Console 口连接在一起，并设置好超级终端。

（3）按住网络设备前面板的 Mode 按钮，插上电源线。当端口 1（2900/3500XL/3550 等）或 STAT（Cisco Catalyst 2940/2950 等）LED 指示灯不再亮后，松开 Mode 按钮，超级终端显示如下内容。

```
The system has been interrupted prior to initializing the
The system has been interrupted prior to initializing the
the flash filesystem, and finish loading the operating
system software:
flash_init
load_helper
bootswitch:
```

(4) 输入 flash_init。

```
switch: flash_init
```

(5) 输入 load_helper。

```
switch: load_helper
switch:
```

(6) 输入 dirflash:。

```
switch: dirflash:
```

(7) 输入 rename flash:config.text flash:config.old,重新命令配置文件。

```
switch: rename flash:config.text flash:config.old
switch:
!--- The config.text file contains the password
!--- definition.
```

(8) 输入 boot,重新启动系统。

```
switch: boot
```

(9) 输入 n,忽略系统初始配置。

```
Continue with configuration dialog? [yes/no]: n
!--- Type "n" for no.
Press RETURN to get started.
!--- Press Return or Enter.
Switch>
!--- The Switch> prompt is displayed.
```

(10) 输入 enable,进入 enable 模式。

```
Switch>enable
Switch#
```

(11) 输入 rename flash:config.old flash:config.text,将配置文件重命名为原始名称。

```
Switch# rename flash:config.old flash:config.text
Destination filename [config.text]
!--- Press Return or Enter.
Switch#
```

(12) 输入 copy flash:config.text system:running-config,将配置文件复制至内存。配置文件被重新装载。

```
Switch#copy flash:config.text system:running-config
Destination filename [running-config]?
!--- Press Return or Enter.
1131 bytes copied in 0.760 secs
Switch#
```

(13) 修改密码。

```
Switch#configure terminal
Switch(config)#no enable secret
!--- This step is necessary if the switch had an enable secret
!--- password.
Switch(config)#enable password Cisco
Switch#(config)#^Z
!--- Use Ctrl-Z.
```

(14) 输入 write memory,将当前运行配置写入配置文件。

```
switch#write memory
Building configuration...
[OK]
Switch#
```

6.5.2 路由器密码恢复

路由器密码恢复步骤如下。

(1) 关掉路由器电源,利用 Console 线将计算机的串行口与路由器的 Console 口连接在一起,并设置好超级终端。

(2) 如果仍然可以访问路由器,输入 show version 命令,并记录配置寄存器的原始值,通常为 0x2102 或 0x102。如果由于遗忘了登录或 TACACS 密码而不能访问路由器,可以将寄存器设置为 0x2102。

```
Router>enable
Password:
Password:
Password:
% Bad secrets
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(7)T, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 07-Dec-99 02:21 by phanguye
Image text-base: 0x80008088, data-base: 0x80C524F8
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Configuration register is 0x2102
Router>
```

(3) 打开路由器的电源,在 60 秒内按下键盘上的 Break 键,使路由器进入 rommon 模式。

(4) 在 rommon 1>提示符下输入 confreg 0x2142,从 Flash 引导,但不装载配置文件。

```
rommon 1 > confreg 0x2142
You must reset or power cycle for new config to take effect
```

(5) 在 rommon 2>提示符下输入 reset,路由器重新引导,并且忽略已经保存的配置文件。

```
rommon 2 > reset
```

(6) 在每个问题后输入 no 或按 Ctrl+C 键,跳过初始设置程序。

(7) 在 Router>提示符下输入 enable,将进入 enable 模式,并看到 Router#提示符。

```
Router>enable
Router#
```

(8) 输入 configure memory 或 copy startup-config running-config 将复制 NVRAM 至内存,不要输入 configure terminal。

```
Router#copy startup-config running-config
```

(9) 输入 write terminal 或 show running-config,查看路由器配置,以及处于加密或非加密状态下的密码(如 enable 密码、enable secret 密码、vty 密码、console 密码等)。非加密密码可以继续使用,但如果是加密密码则需要另外更换。

```
Router#show running-config
```

(10) 输入 configure terminal,进入配置模式,提示符改变为 hostname(config)#。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
00:01:54: %SYS-5-CONFIG_I: Configured from console by console
Router(config)#
```

(11) 输入 enable secret <password>修改 enable secret 密码。

```
Router(config)#enable secret cisco
Router(config)#^Z
```

(12) 进入每个使用的接口,输入 no shutdown 命令,启动该端口。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
00:02:14: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:02:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
to up
Router(config-if)#interface Serial0/0
Router(config-if)#no shutdown
Router(config-if)#
```

(13) 输入 config-register 0x2102,或者记录的配置寄存器的原始值。

```
Router(config)#config-register 0x2102
```

(14) 按 Ctrl+Z 键或 End 键,离开配置模式。提示符改变为 hostname#。

```
Router(config)#^Z
00:03:20: %SYS-5-CONFIG_I: Configured from console by console
```

(15) 输入 write memory 或 copy running-config startup-config,提交修改。

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

6.5.3 安全设备密码恢复

安全设备密码恢复步骤如下。

(1) 关掉路由器电源,利用 Console 线将计算机的串行口与安全设备的 Console 口连接在一起,并设置好超级终端。

(2) 打开路由器的电源,显示启动信息的时候,按 Esc 键,使安全设备进入 rommon 模式。

(3) 在 rommon 1>提示符下输入 confreg,从 Flash 引导,但不装载配置文件。

```
rommon 1 > confreg
```

显示当前配置注册值,并且会提示 Do you wish to change this configuration。

```
Current Configuration Register: 0x00000011
Configuration Summary:
boot TFTP image, boot default image from Flash on netboot failure
Do you wish to change this configuration? y/n [n]:
```

(4) 记录当前配置的注册值,以备稍后恢复,根据提示输入 y 更改注册值。

(5) 除了 disable system configuration 输入 y,其他设置保持默认值即可。

(6) 重新启动设备,输入 boot 命令即可,设备会加载默认的配置而不加载 startup-config 文件。

```
Rommon #2> boot
```

(7) 设备启动后进入特权模式。当系统提示输入密码,直接按 Enter 键即可。

```
Hostname>enable
```

(8) 输入 copy startup-config running-config 将复制 NVRAM 至内存,不要输入 configure terminal。

```
Hostname#copy startup-config running-config
```

(9) 输入 write terminal 或 show running-config,查看路由器配置,以及处于加密或非加密状态下的密码(如 enable 密码、enable secret 密码、vty 密码、console 密码等)。非加密

密码可以继续使用，但如果是加密密码则需要另外更换。

```
Hostname# show running-config
```

（10）输入 configure terminal，进入配置模式。

```
Hostname# configure terminal
```

（11）配置新密码，对于安全产品来说这步是必要的。

```
Hostname(config) # password password
Hostname(config) # enable password password
Hostname(config) # username name password password
```

（12）通过以下命令更改注册值，并且在下一次重启时加载 startup-config 启动。这里所输入的注册值即为第 4 步所记录的值。

```
Hostname(config) # config-register volue
```

（13）保存新配置到 startup-config 文件。

```
Hostname(config) # copy running-config startup-config
```

6.6　CiscoWorks LMS

CiscoWorks LMS 是 Cisco 公司推出的专门为中小企业设计的管理软件，使用 SNMP 作为核心协议的网络管理系统。

6.6.1　安装 CiscoWorks LMS

在开始安装 CiscoWorks LMS 前，除对 Windows 系统进行设置外，还应安装其他所需组件和支持工具，例如 Java 插件。

1. 安装系统需求

CiscoWorks LMS 的安装和运行对服务器具有一定的要求，在安装之前，必须保证服务器至少满足如下配置。

（1）硬件要求

硬件要求如下。

① Pentium 4 2.0GHz 以上 CPU。

② 2048MB 以上内存。

③ 2GB 以上自由磁盘空间。

④ DVD-ROM 驱动器。

⑤ 系统缓存大于等于内存容量。

⑥ 10/100Mbps 自适应网卡。

（2）软件需求

软件要求如下。

① 安装 Windows Server 2003，并安装 SP1 和 R2 补丁包。

② 正确配置 IP 地址、子网掩码和默认网关等。

③ 采用 NTFS 文件系统，不能安装于 FAT 文件系统。

④ Windows Server 2003 为独立服务器，不能设置为主域控制器。

⑤ 安装网卡驱动程序，设置 IP 地址，并检查被管理设备的连通性。

⑥ 安装 Internet Explorer 6.0 或以上版本。

⑦ 安装 Microsoft VM，升级到最新版本。

注意：网管服务的主机名和 IP 地址一旦确定，在安装完 CiscoWorks 系统后不要更改，因其涉及的设置项目很多，请一定要注意。

2. 安装前准备工作

(1) 安装 Java

因为使用 CiscoWorks 管理网络设备，需要使用支持 Java 的 IE 浏览器，因此需要在准备安装 CiscoWorks 的计算机上，安装 Java 程序。Java 软件包可以在 http://www.sun.com.cn 网站上下载并安装。

(2) IE 浏览器设置

IE 浏览器设置步骤如下。

① 打开 IE 浏览器，依次选择 IE 菜单"工具"→"Internet 选项"命令，打开图 6-45 所示的"Internet 属性"对话框。

② 单击"设置"按钮，显示图 6-46 所示的"设置"对话框。选中"每次访问此页时检查"单选按钮，设置"使用的磁盘空间"大于 6MB。

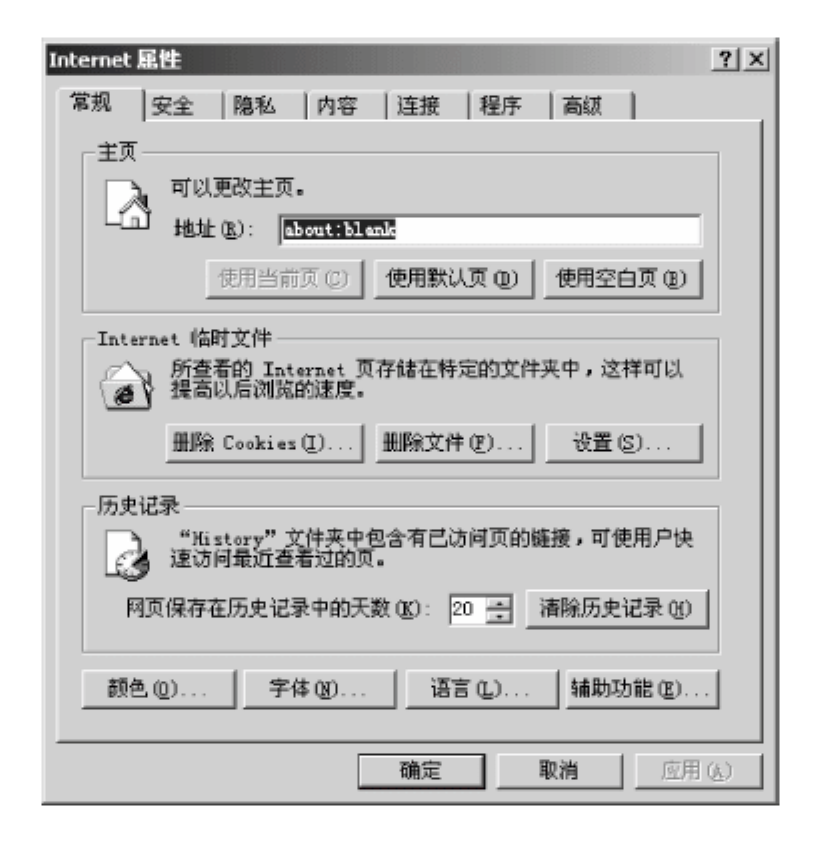


图 6-45 "Internet 属性"对话框



图 6-46 "设置"对话框

③ 单击"确定"按钮，返回"Internet 属性"对话框。单击"字体"按钮，显示图 6-47 所示的"字体"对话框。在"网页字体"列表中，选择 Microsoft Sans Serif 选项。

④ 在"Internet 属性"对话框中选择"高级"选项卡，选中 Microsoft VM 中的"启用 Java 控制台(需要重启动)"复选框，如图 6-48 所示。

⑤ 最后，单击"确定"按钮保存设置。

3. 安装 CiscoWorks LMS

在 CiscoWorks LMS 的安装过程中，需要根据需要选择所需要的组件，以及一些基本设置，例如管理员密码等。这里以安装 CiscoWorks LMS 3.0 为例进行介绍，主要操作步骤如下。



图 6-47 “字体”对话框



图 6-48 “高级”选项卡

(1) 将 CiscoWorks LMS 安装光盘插入光驱,显示图 6-49 所示的安装界面。

(2) 单击 Install 按钮,并连续单击 Next 按钮,显示图 6-50 所示的 Software License Agreement 对话框。

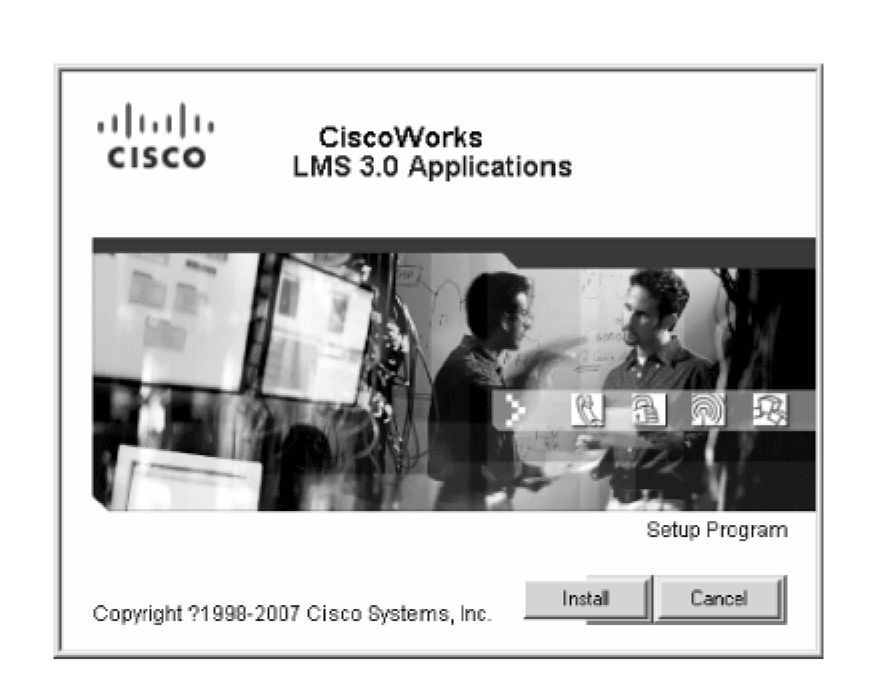


图 6-49 CiscoWorks LMS 3.0 安装界面



图 6-50 Software License Agreement 对话框

(3) 单击 Accept 按钮,显示图 6-51 所示的 Setup Type 对话框,选中 Typical installation 单选按钮,使用典型安装类型即可。

(4) 单击 Next 按钮,显示图 6-52 所示的 Select Applications 对话框。根据需要选中所要安装的组件,这里选择除 Device Fault Manager 3.0 HPOV-Netview adapters 外的所有组件。需要注意的是,Device Fault Manager 3.0 HPOV-Netview adapters 组件和 Device Fault Manager 3.0 组件不能同时安装。

(5) 单击 Next 按钮,显示图 6-53 所示的 Licensing Information 对话框。选中 License File Location 单选按钮,并单击 Browse 按钮,浏览并选中许可证文件。

(6) 单击 Next 按钮,显示图 6-54 所示的 System Requirements 对话框。检查系统是否符合 CiscoWorks LMS 的最低要求,在 Available 列中,显示的是当前系统的检测内容,在 Required 列中,显示的是软件的最低要求。

(7) 单击 Next 按钮,显示图 6-55 所示的 Enter the Admin Password 对话框。在 User Admin Password 和 Confirm Password 文本框中,分别输入管理员 Admin 的密码和确认密码。

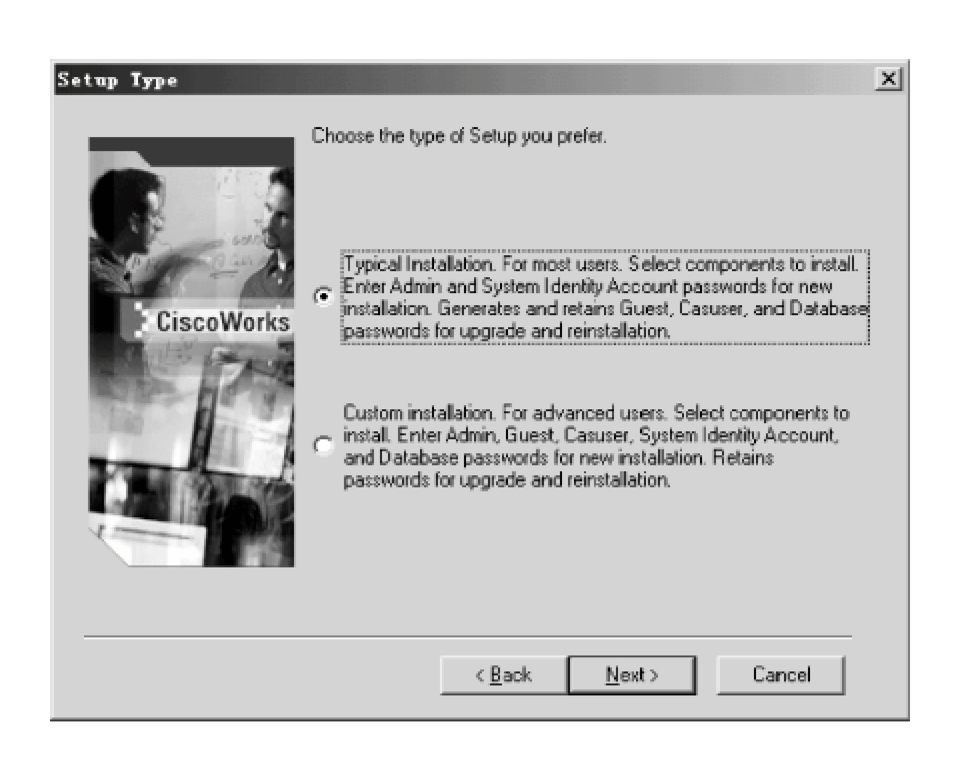


图 6-51　Setup Type 对话框



图 6-52　Select Applications 对话框



图 6-53　Licensing Information 对话框

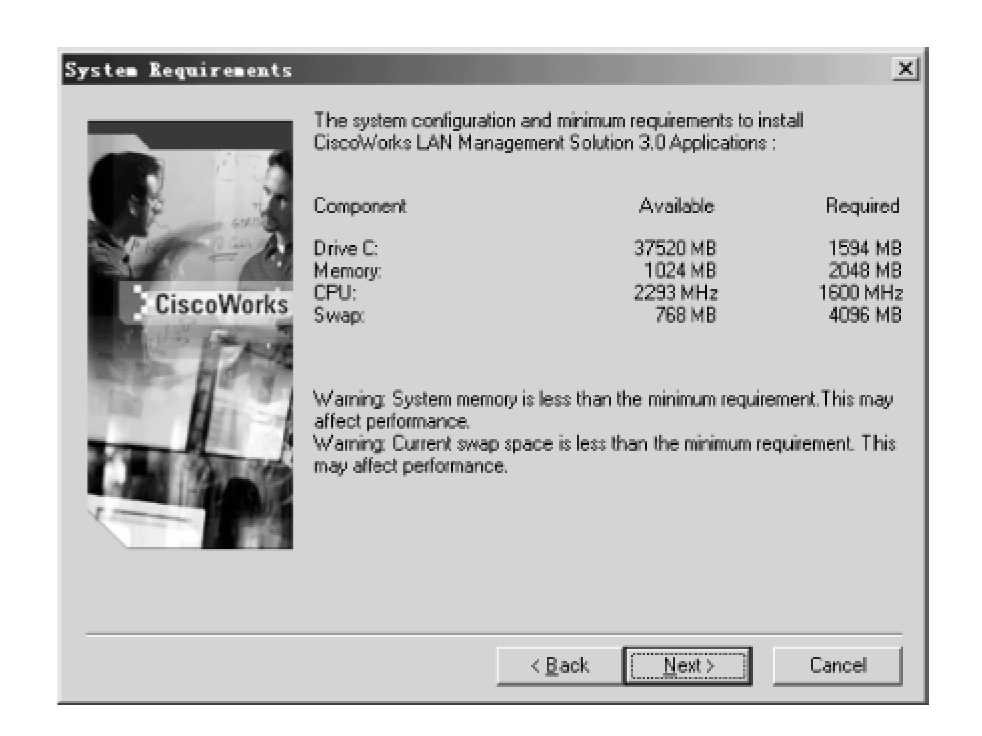


图 6-54　System Requirements 对话框

（8）单击 Next 按钮，显示图 6-56 所示的 Enter the System Identity Account Password 对话框。分别在 System Identity Account Password 和 Confirm Password 文本框中，输入系统标识密码。

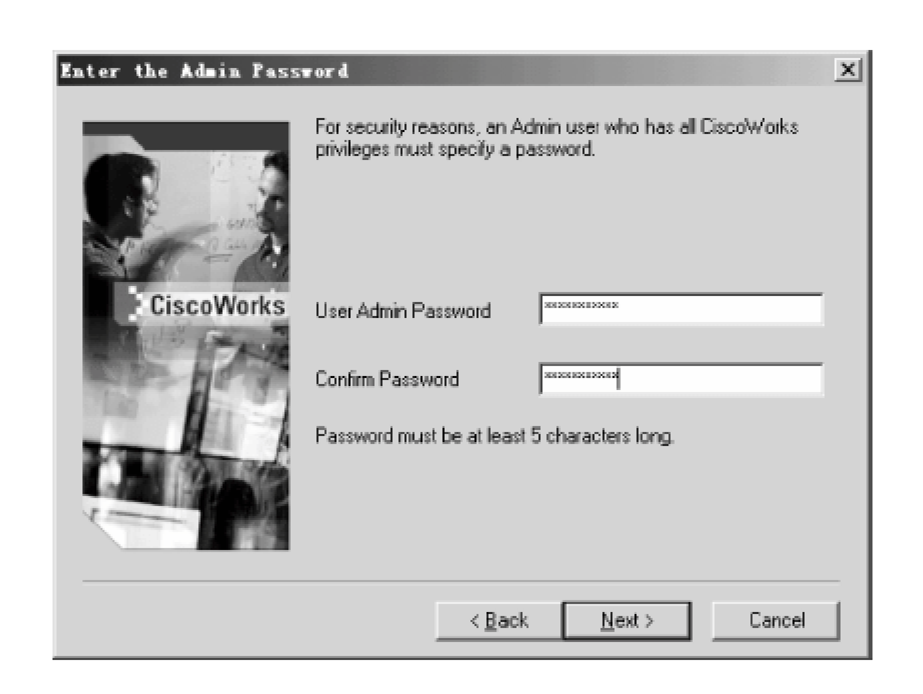


图 6-55　Enter the Admin Password 对话框

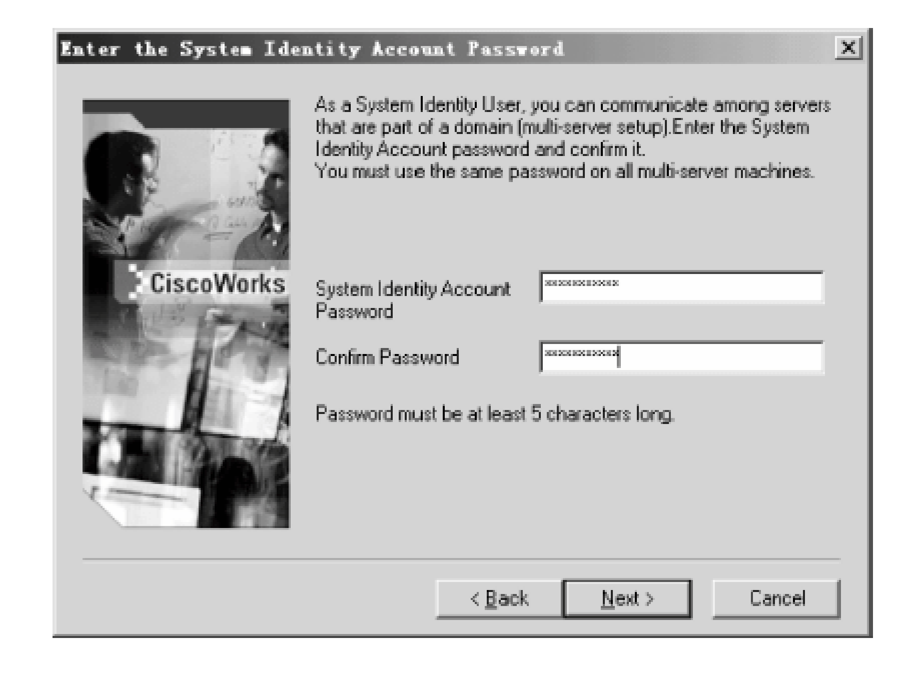
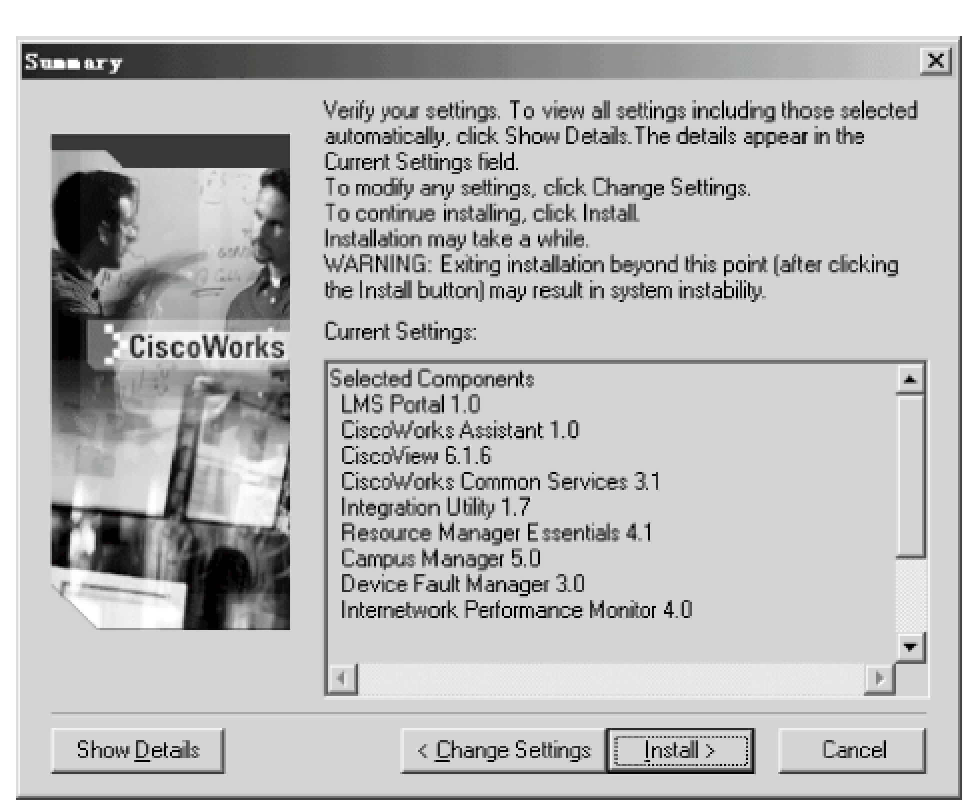
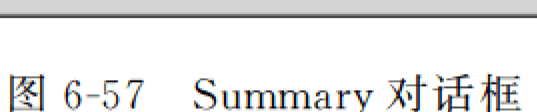


图 6-56　Enter the System Identity Account Password 对话框

（9）单击 Next 按钮，显示图 6-57 所示的 Summary 对话框，查看前面的设置是否正确。

（10）单击 Install 按钮，开始安装 CiscoWorks LMS。需要注意的是，这个过程需要比较长的时间。安装完成后，显示图 6-58 所示的 Information 对话框，显示安装结果。




图 6-57　Summary 对话框

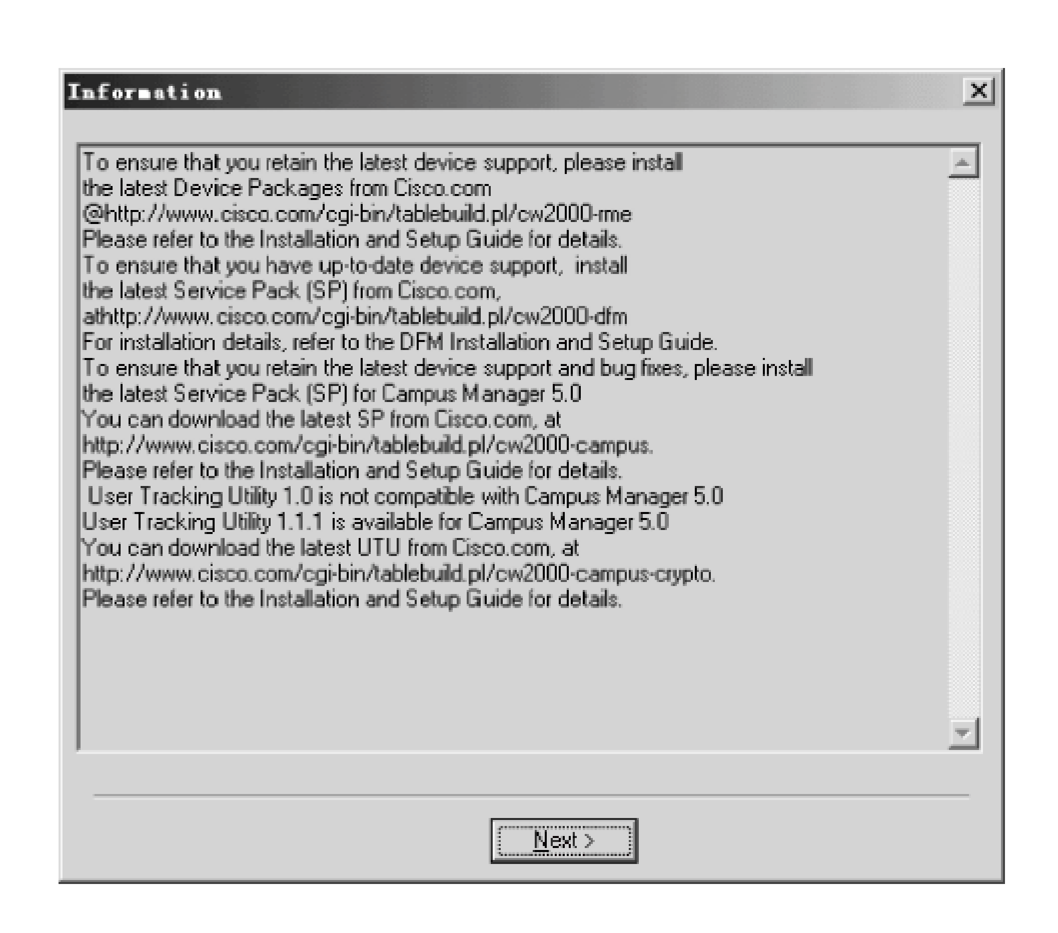


图 6-58　Information 对话框

（11）单击 Next 按钮，显示图 6-59 所示的 Restart 对话框，提示需要重新启动计算机。

（12）单击 Finish 按钮，重新启动计算机完成安装。

注意：在 CiscoWorks 安装完成后，还需要安装 CiscoWorks 的补丁包，具体安装步骤与 CiscoWorks 基本相同，这里就不再赘述。

4. 客户端配置

CiscoWorks 安装完成以后，即可以在网络中的任何一台计算机上进行管理。由于 CiscoWorks 的功能非常多而且强大，因此，这里只介绍一些常用且较重要的功能。

客户端计算机在连接 CiscoWorks 时需要运行 Java 脚本程序。由于 IE 浏览器的安全级别默认设置为“高”，此时会禁止 Java 脚本程序的运行，导致界面不能显示。因此，需要按如下步骤设置。

打开 IE 浏览器，依次选择“工具”→“Internet 选项”命令，在“Internet 选项”对话框中选择“安全”选项卡，单击“自定义级别”按钮显示“安全设置”对话框，在“脚本”选项区域中，在“Java 小程序脚本”和“活动脚本”下均选中“启用”单选按钮，如图 6-60 所示。

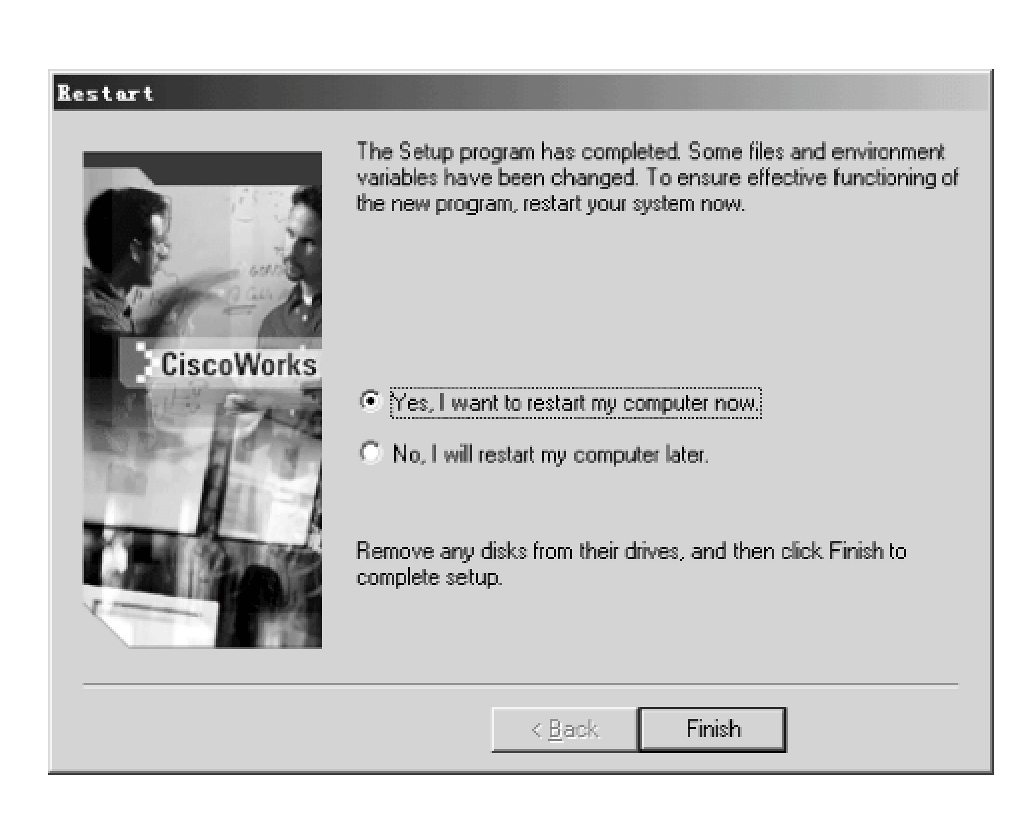


图 6-59　Restart 对话框

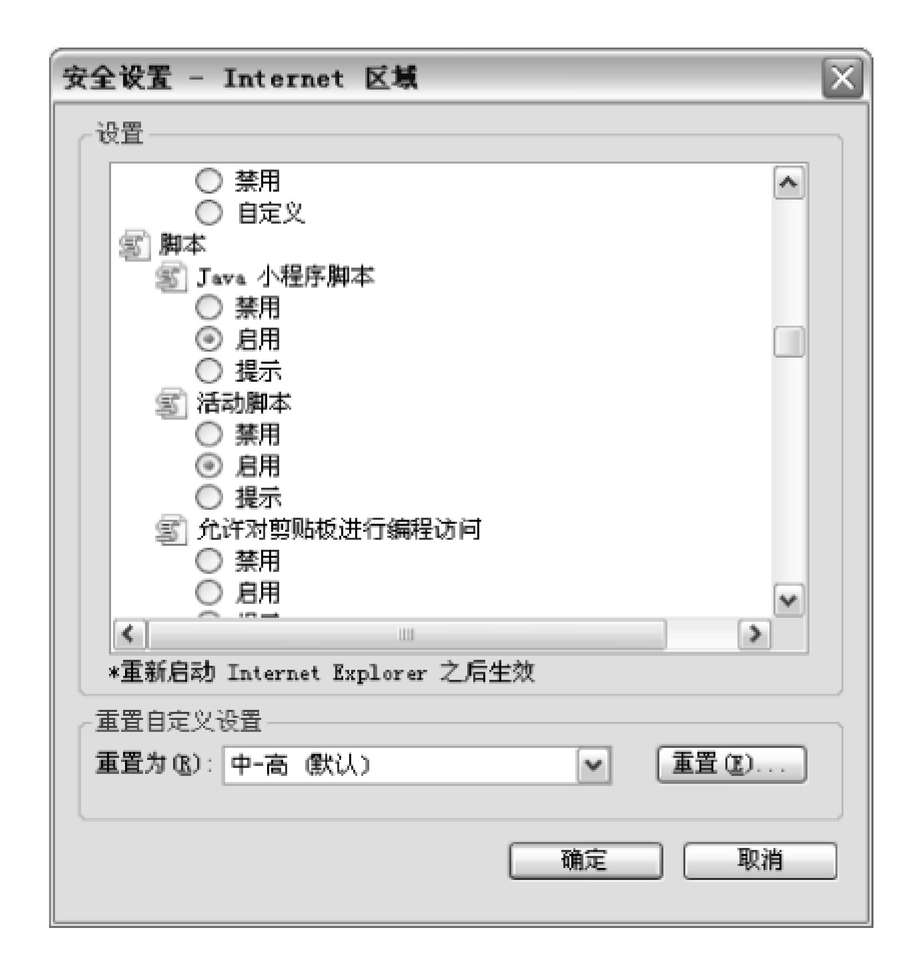


图 6-60　“安全设置”对话框

另外,IE 浏览器还必须允许弹出窗口,或者只允许 CiscoWorks 服务器站点弹出窗口,否则,将不能正确显示。

5. 登录 CiscoWorks

在 CiscoWorks 服务器上,可以依次选择"开始"→"程序"→CiscoWorks→CiscoWorks 命令,登录 CiscoWorks。

而在客户端计算机,则可以打开 IE 浏览器,在地址栏中输入 http://ciscoworks 服务器 IP 地址:1741,即可登录 CiscoWorks,如图 6-61 所示。

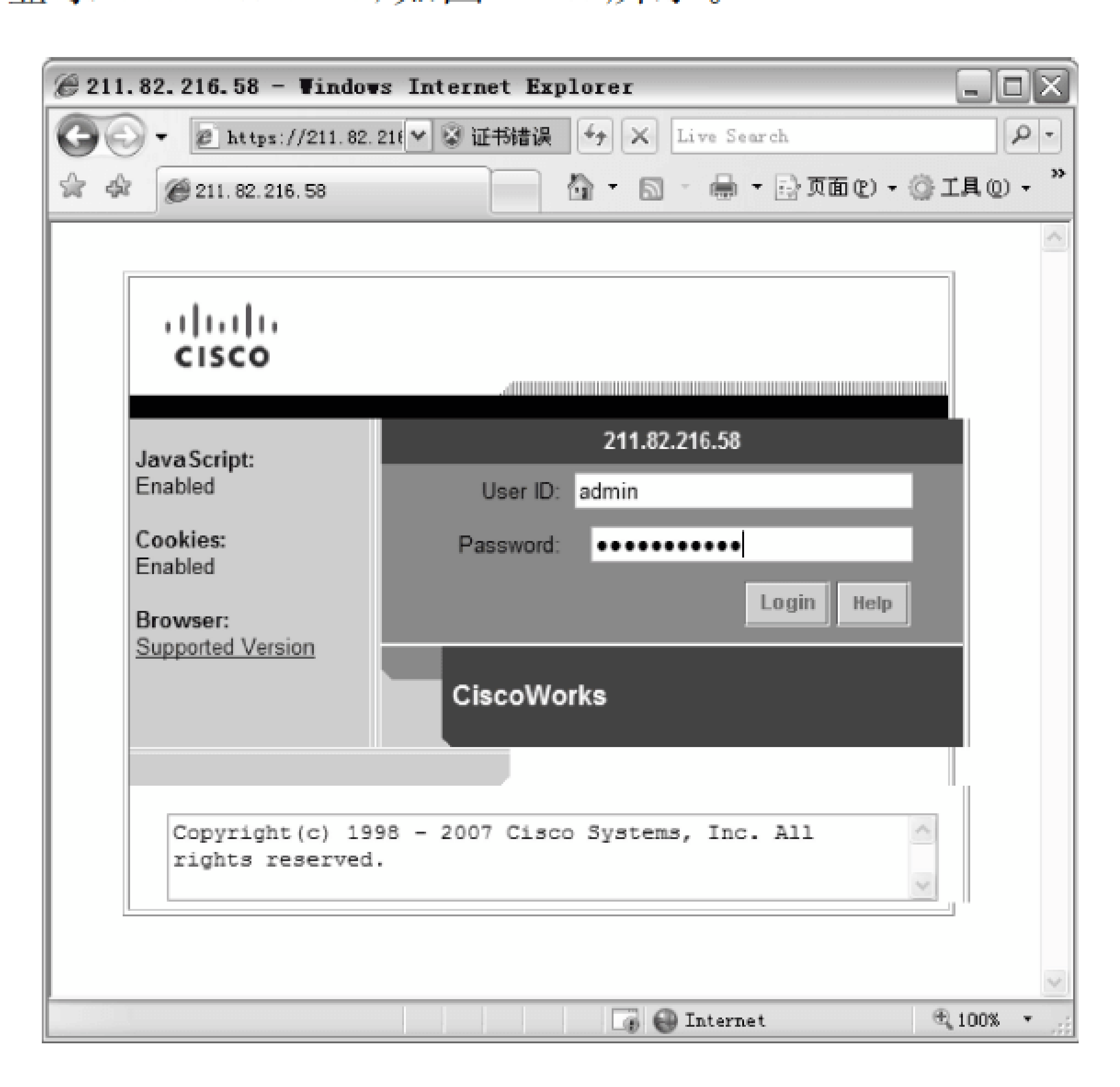


图 6-61　客户端登录 CiscoWorks

6.6.2　CiscoWorks 自动搜索网络设备

在 CS 中可以利用设备自动搜索功能,对网络内的设备进行全面自动搜索,避免大量手工输入工作,这也是能够使用 LMS 所有功能的首要条件。自动搜索完毕后,所能管理的设备将自动存入 CS 和 CM 设备管理库,若有特殊设备需要存入设备库,也可以通过 CS 的设备管理来手动添加。

(1) 在 CiscoWorks 主页的 CS 面板上,选择 Device and Credentials 选项卡,在展开的列表中,单击 Device Discovery 链接,显示图 6-62 所示的 Discovery Settings Summary 窗口,显示了当前发现的设备。

(2) 单击左侧的 Device Settings 链接,显示图 6-63 所示的页面,显示了当前自动发现的配置汇总信息。

(3) 单击 Configure 按钮,显示图 6-64 所示的 Module Settings 窗口。根据实际情况选择所使用的发现协议,这里只选中 Cisco Discovery Protocol(CDP)复选框。

(4) 单击 Next 按钮,显示图 6-65 所示的 Seed Device Settings 窗口。设置种子设备的 IP 地址,用作网络发现的起点。在 Seed Devices 列表中,选择 CDP 选项,单击 Add 按钮添加,可添加多个种子设备地址。

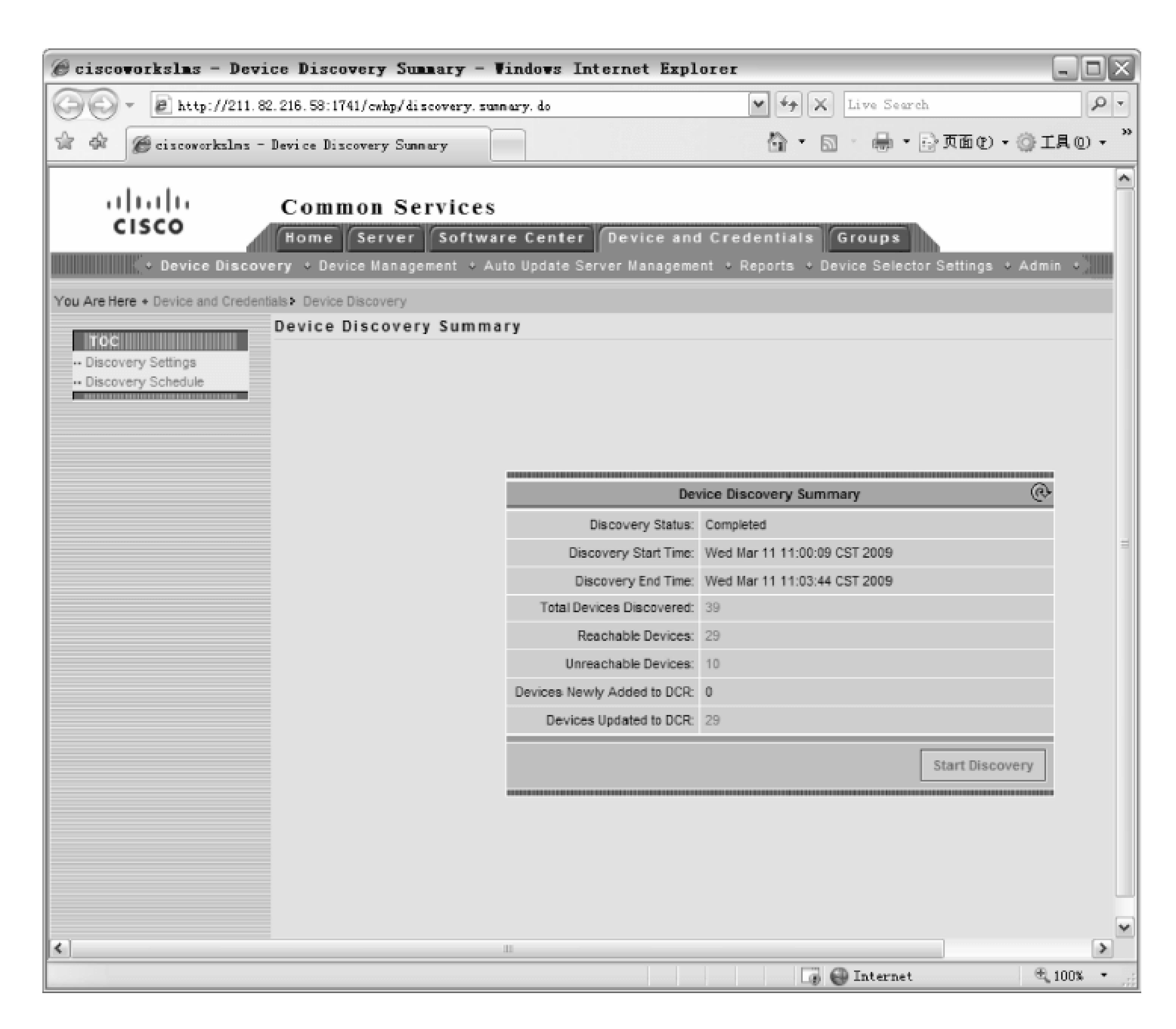


图 6-62　Discovery Settings Summary 窗口

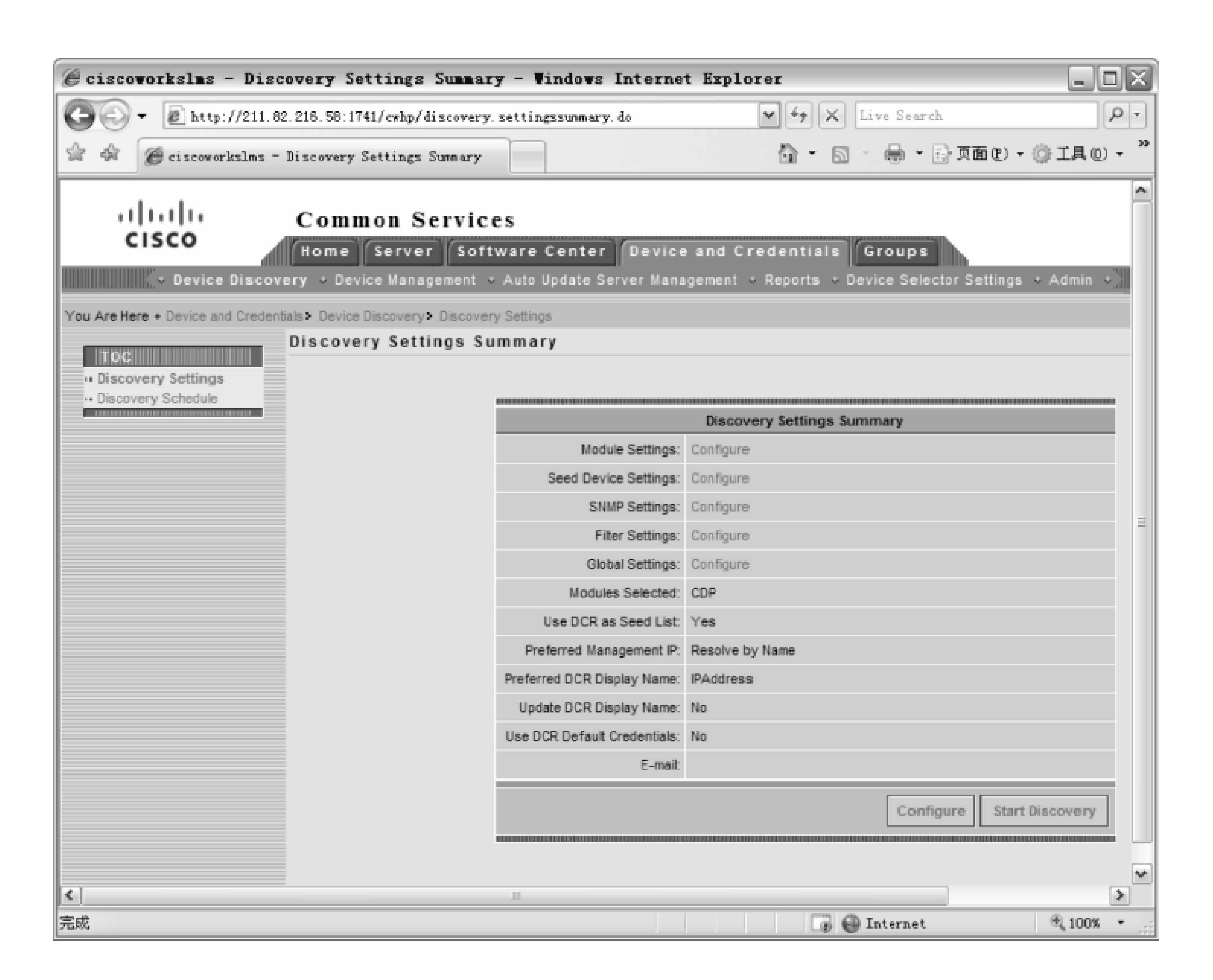


图 6-63　自动发现配置信息

(5) 单击 Next 按钮，显示图 6-66 所示的 SNMP Settings 窗口，选中 v2c 复选框。

(6) 单击 Edit 按钮，显示图 6-67 所示的 SNMPv2 窗口。在 Target 文本框中输入网络中设备的地址，“ * ”表示所有。在 Read Community 文本框中，输入 SNMP 读取字符串，其他设置保持默认值即可。



图 6-64 Module Settings 窗口

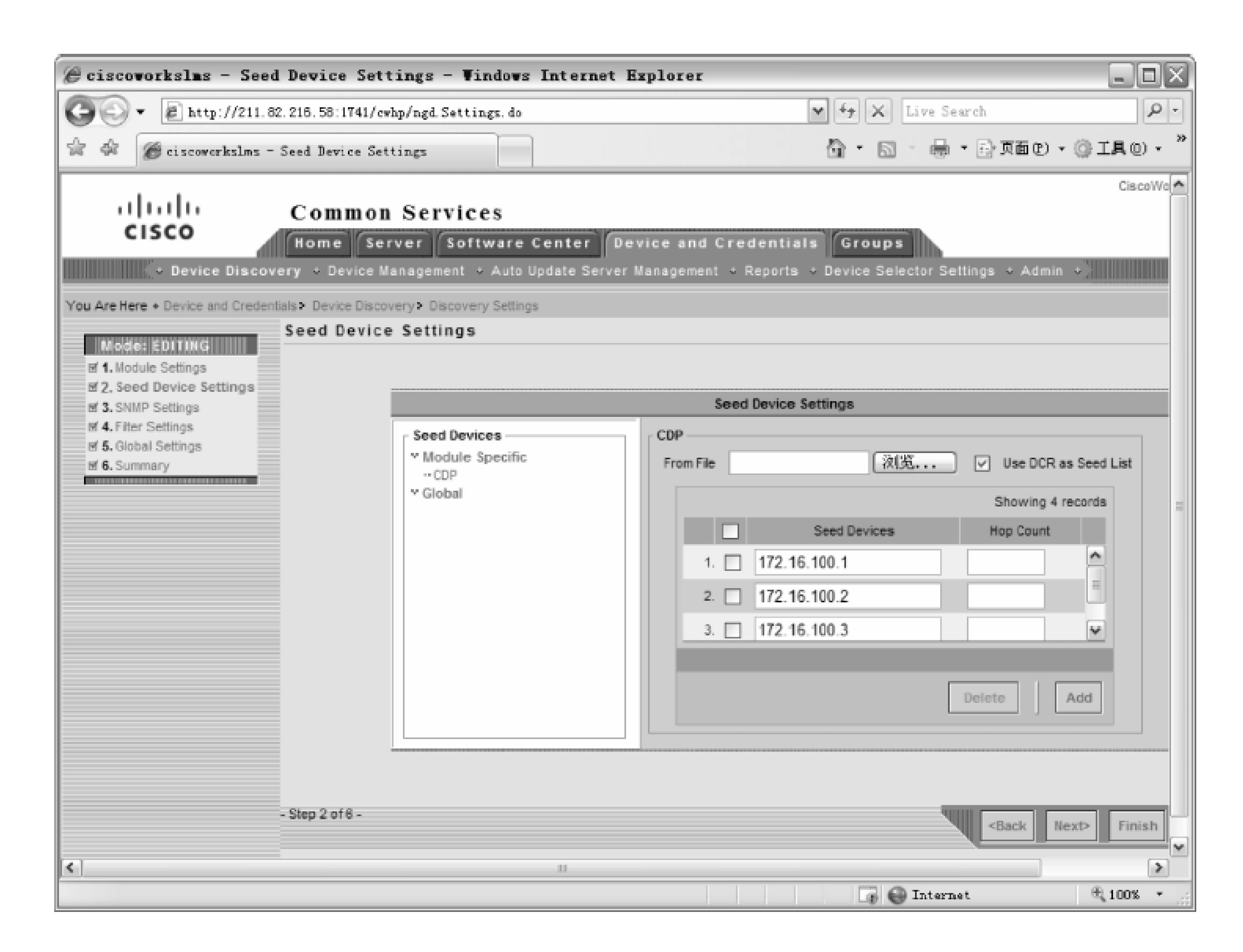


图 6-65 Seed Device Settings 窗口

(7) 单击 OK 按钮，返回 SNMP Settings 窗口，再单击 Next 按钮，显示图 6-68 所示的 Filter Settings 窗口。在 IP Address 文本框中，可添加要搜索的网络设备的 IP 地址范围。如果网络设备不在同一 IP 地址段，可单击 Add 按钮添加不同的 IP 地址范围。

(8) 单击 Next 按钮，显示图 6-69 所示的 Global Settings 窗口。进行常规设置，在 Preferred DCR Display Name 列表中，选择设备的显示名称。在 Preferred Management IP 列表中，选择首选管理 IP 地址。

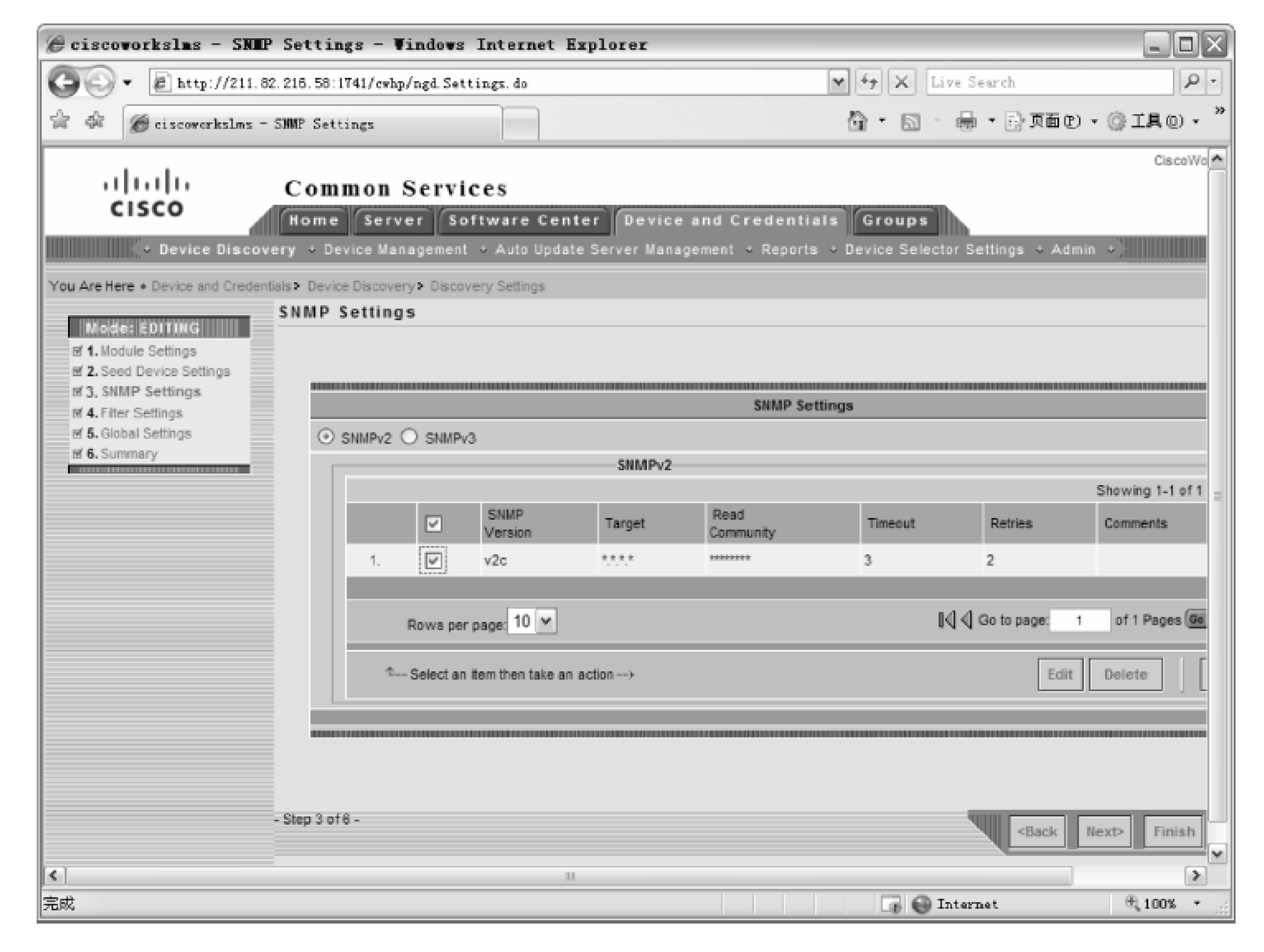


图 6-66 SNMP Settings 窗口



图 6-67 SNMPv2 窗口

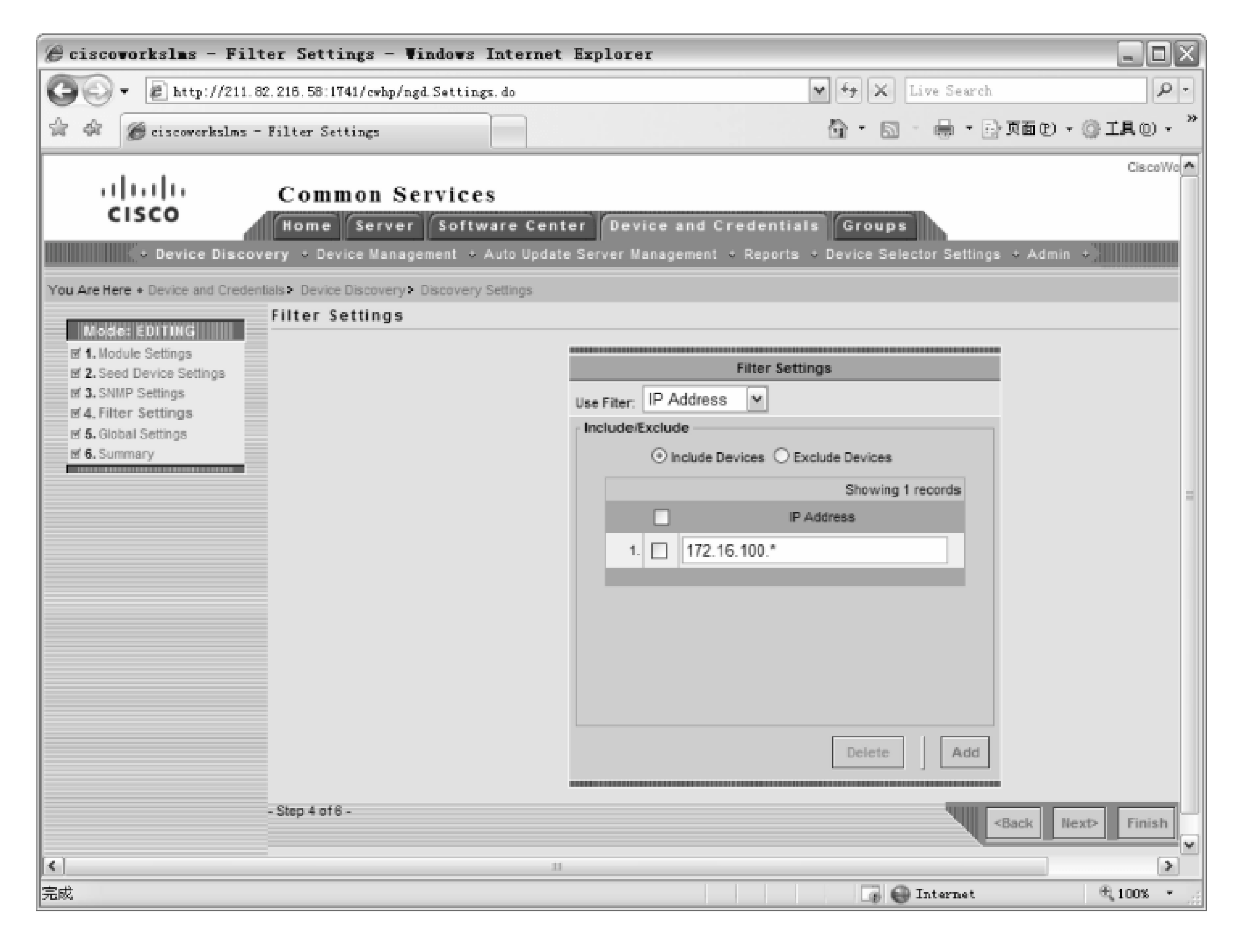


图 6-68 Filter Settings 窗口

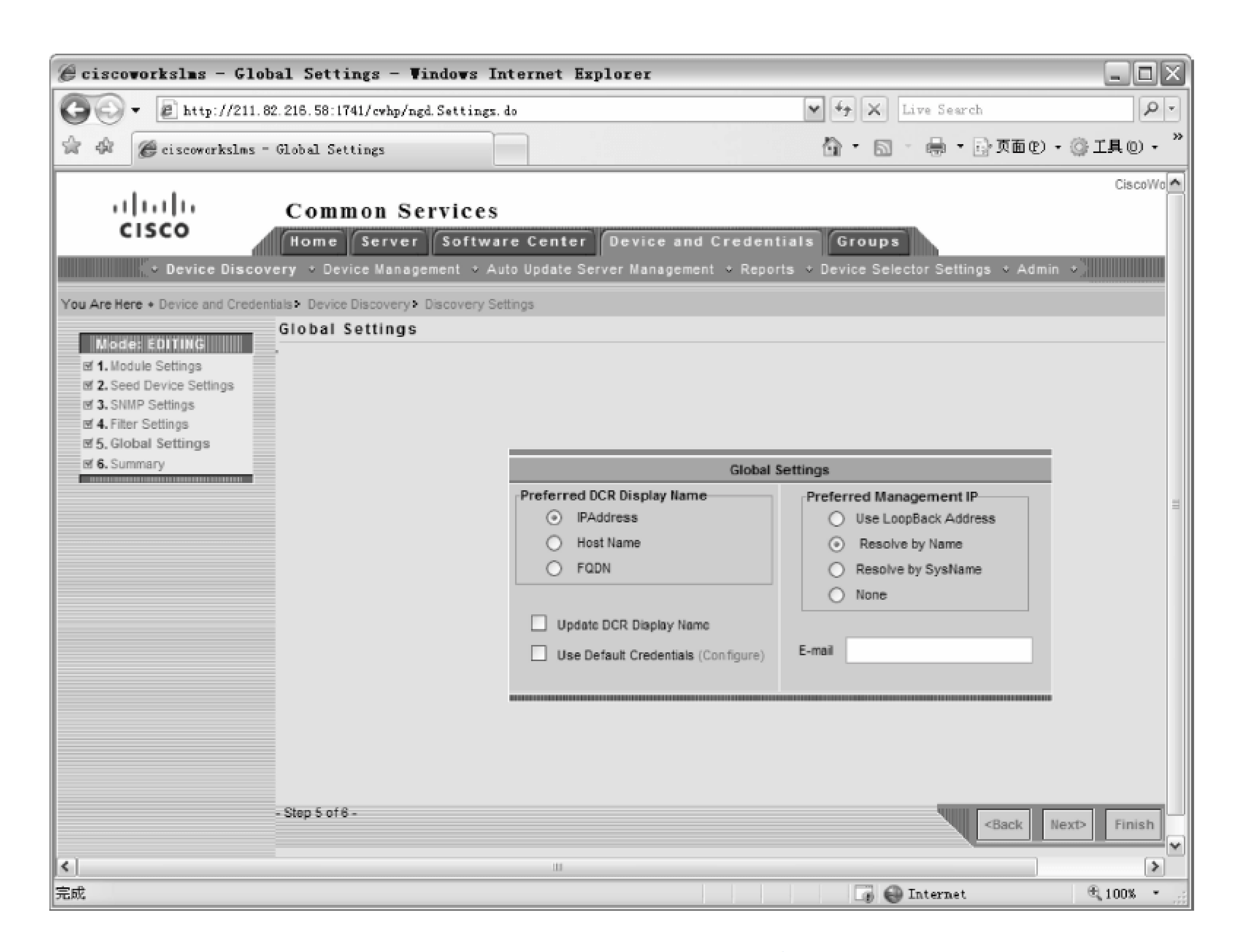


图 6-69 Global Settings 窗口

(9) 单击 Next 按钮，显示图 6-70 所示的 Summary 窗口，显示前面设置的摘要信息。

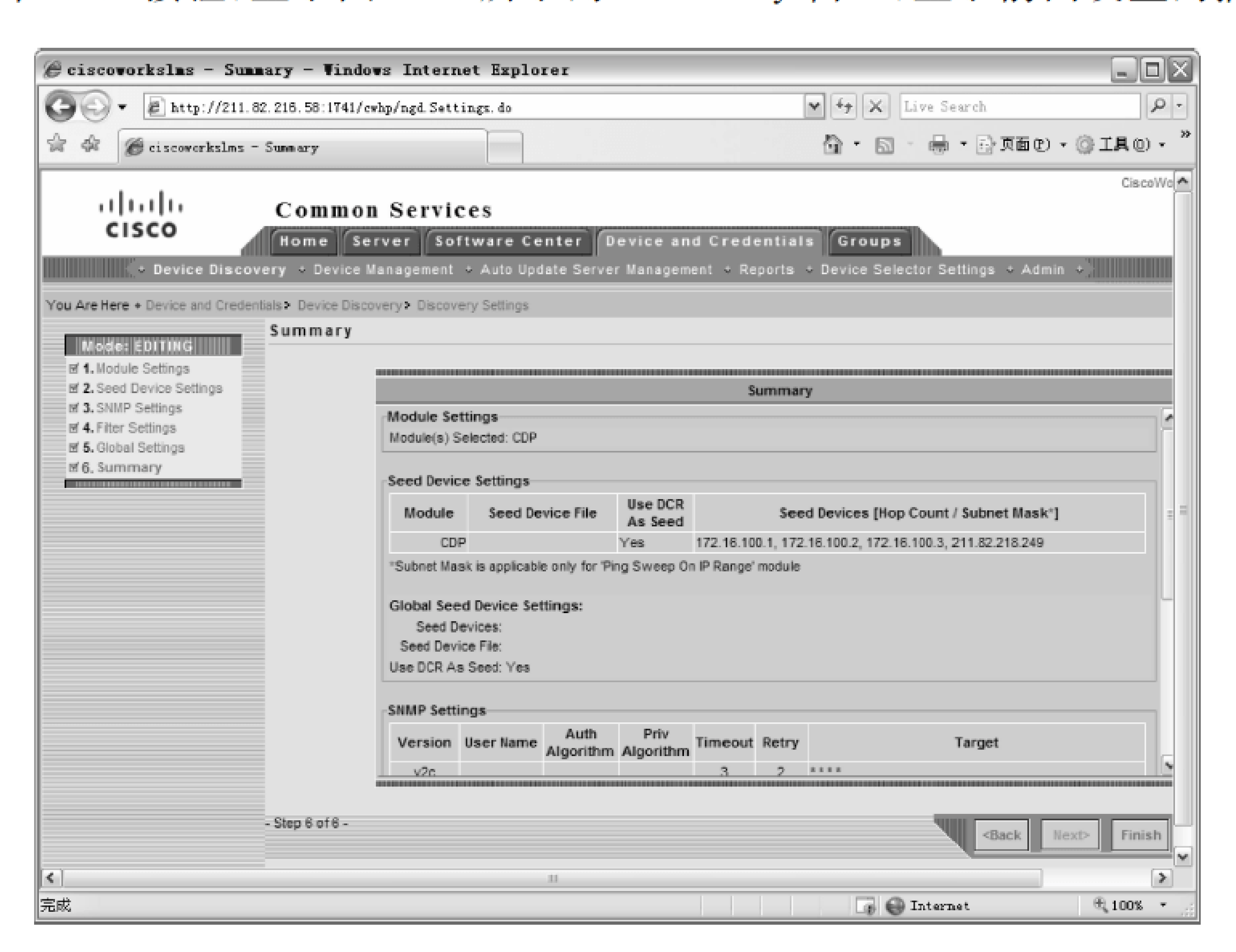


图 6-70 Summary 窗口

(10) 单击 Finish 按钮，返回 Discovery Settings Summary 窗口。单击 Start Discovery 按钮，显示图 6-71 所示的 Info 窗口。

(11) 单击 OK 按钮，即可开始设备的自动发现。发现完成后，显示图 6-72 所示的发现完成窗口。从图中可知，共发现 39 个设备，其中 29 个设备可访问，10 个设备不可访问。



图 6-71　Info 窗口

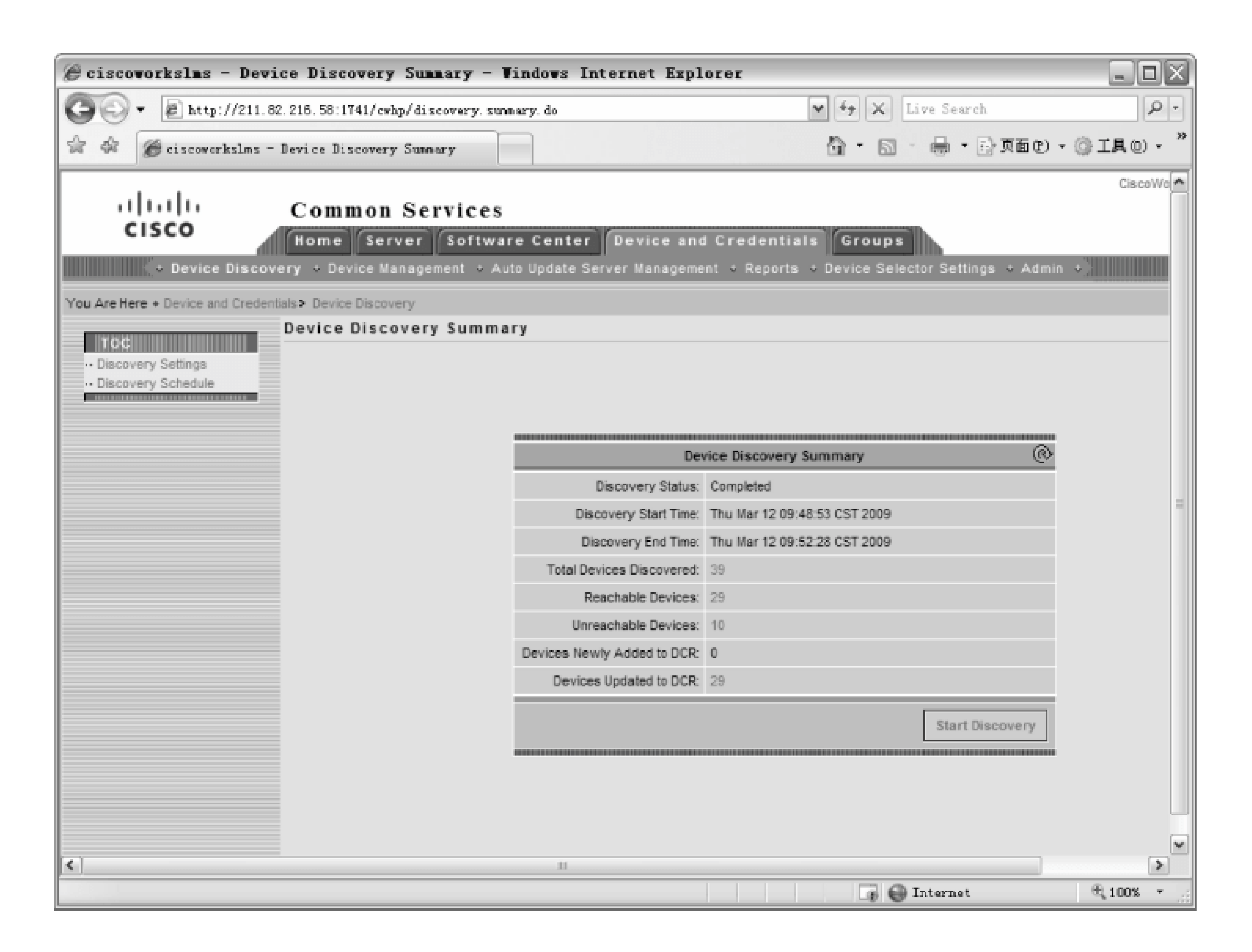


图 6-72　完成设备发现

小知识：如果不能自动搜索到所有设备，可检查设备的配置，然后再次搜索。如果想再次搜索，则可单击 Start Device Discovery 链接。

所有搜索到的设备会自动保存到 Common Services 中的 Device and Credentials 列表中。在 Device Management 窗口中，展开 All Devices 目录，即可查看所有搜索到的设备，如图 6-73 所示。

6.6.3　向 CiscoWorks 中手动添加网络设备

虽然使用自动搜索设备，可以将大多数的网络设备自动添加到 CiscoWorks 中，但有些设备可能会因为种种原因，不能被自动搜索到。为了管理这些设备，需要使用手动添加设备的方法将这些设备添加到 CiscoWorks 中。

（1）在 Common Services 窗口中，选择 Device and Credentials 选项卡，单击 Device Management 链接，显示图 6-74 所示的 Device Management 窗口。

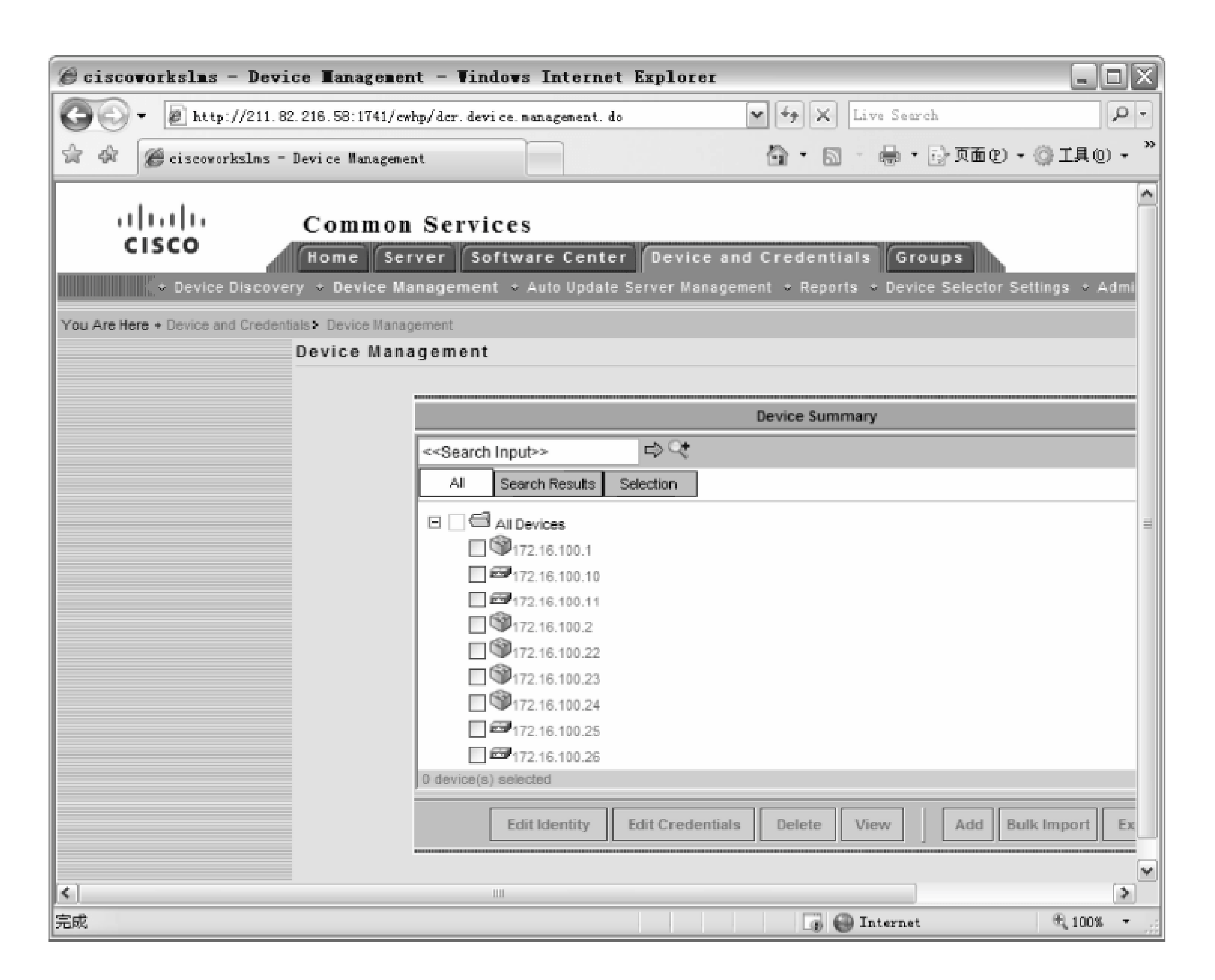


图 6-73　已搜索到的设备

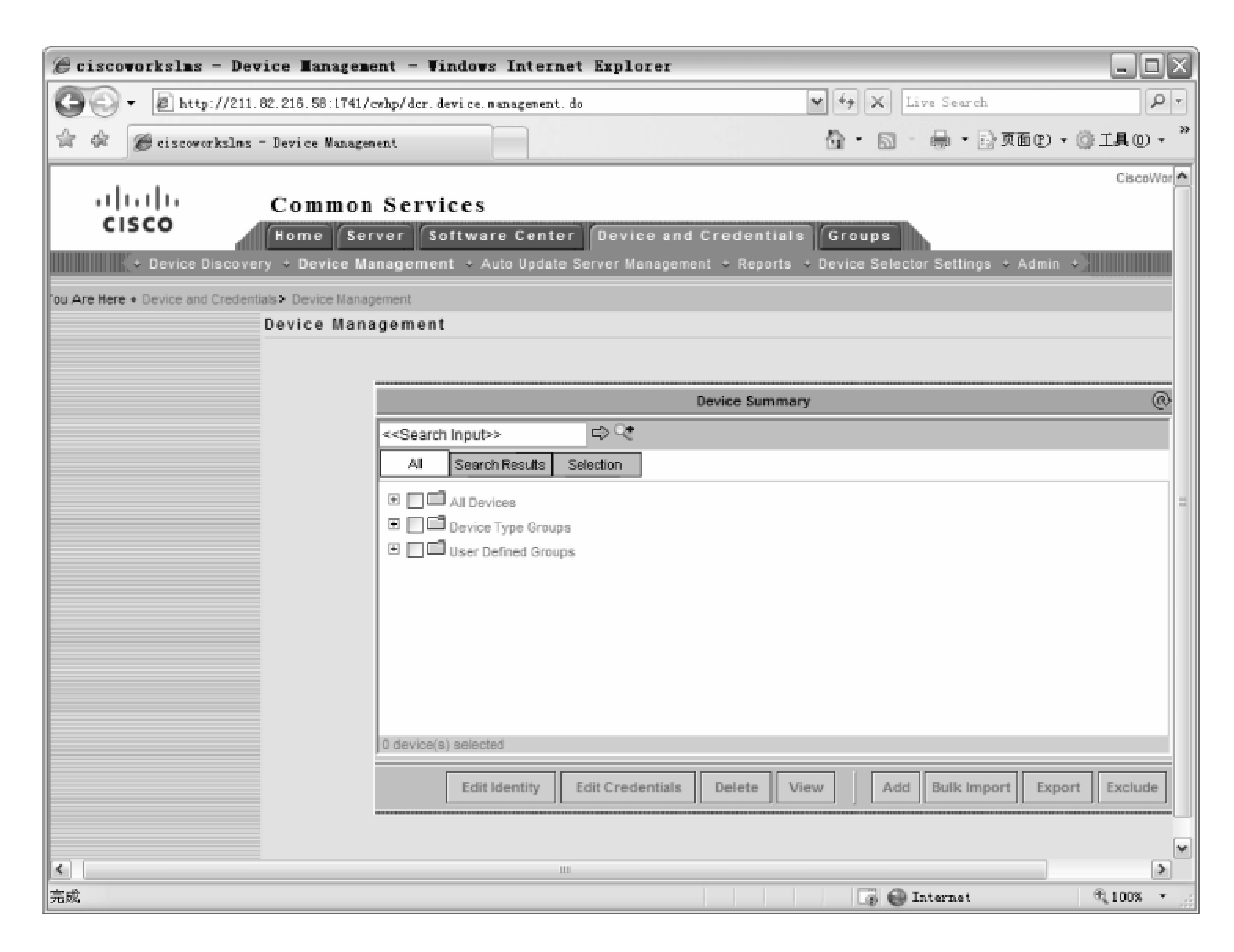


图 6-74　Device Management 窗口

(2) 单击 Add 按钮，显示图 6-75 所示的 Device Properties 窗口，设置要添加的设备属性。

(3) 单击 Select 按钮，显示图 6-76 所示的 Device Type 窗口，选择要添加的设备类型，例如，要添加交换机，则可展开 Switches and Hubs 项，在列表中选择要添加的交换机类型。

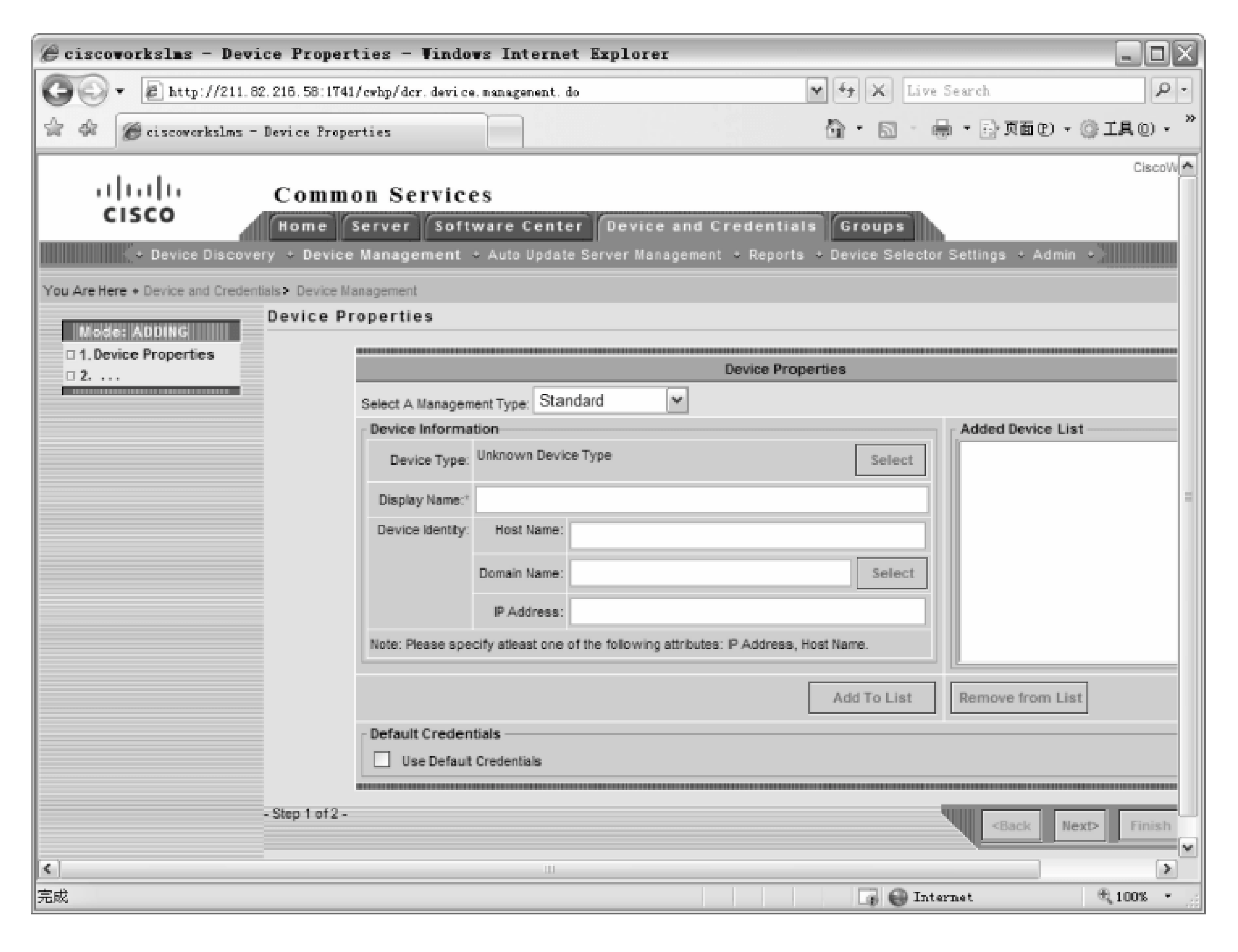


图 6-75　Device Properties 窗口

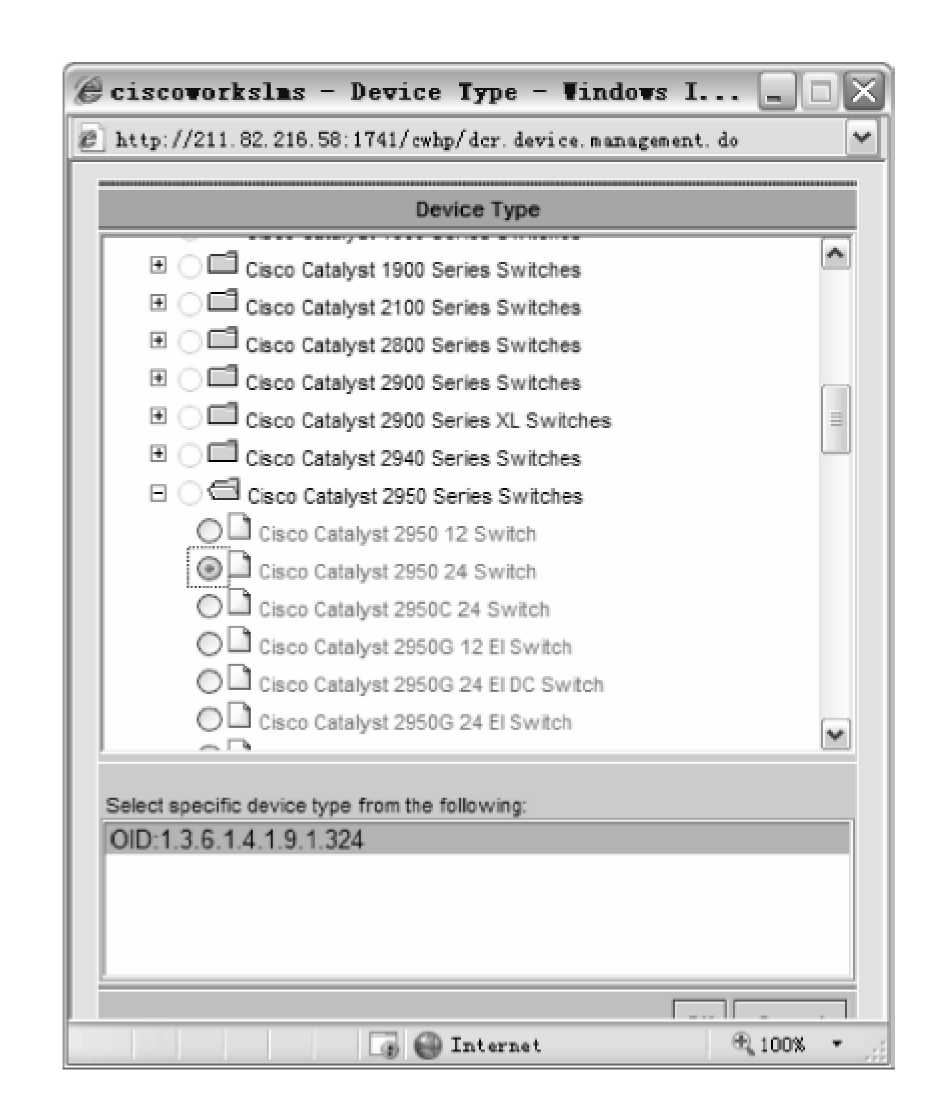


图 6-76　Device Type 窗口

(4) 按键盘上的 Tab 键选择 OK 按钮，添加并返回 Device Properties 窗口。在 Display Name 文本框中输入该设备的显示名称，在 IP Address 文本框中输入该设备的 IP 地址，如图 6-77 所示。单击 Add To List 按钮，添加到 Added Device List 列表框中。重复操作，可添加多个设备。

(5) 选择完设备后，单击 Next 按钮，显示图 6-78 所示的 Standard Credentials 窗口，在 Primary Credentials 选项区域中，分别输入登录交换机时的口令。

注意： 如果要同时添加多个设备，在此处设置的口令信息将会同时应用于这些设备，因此，必须确保各设备的口令相同。否则，应逐个添加设备，或者在添加后再进行修改。

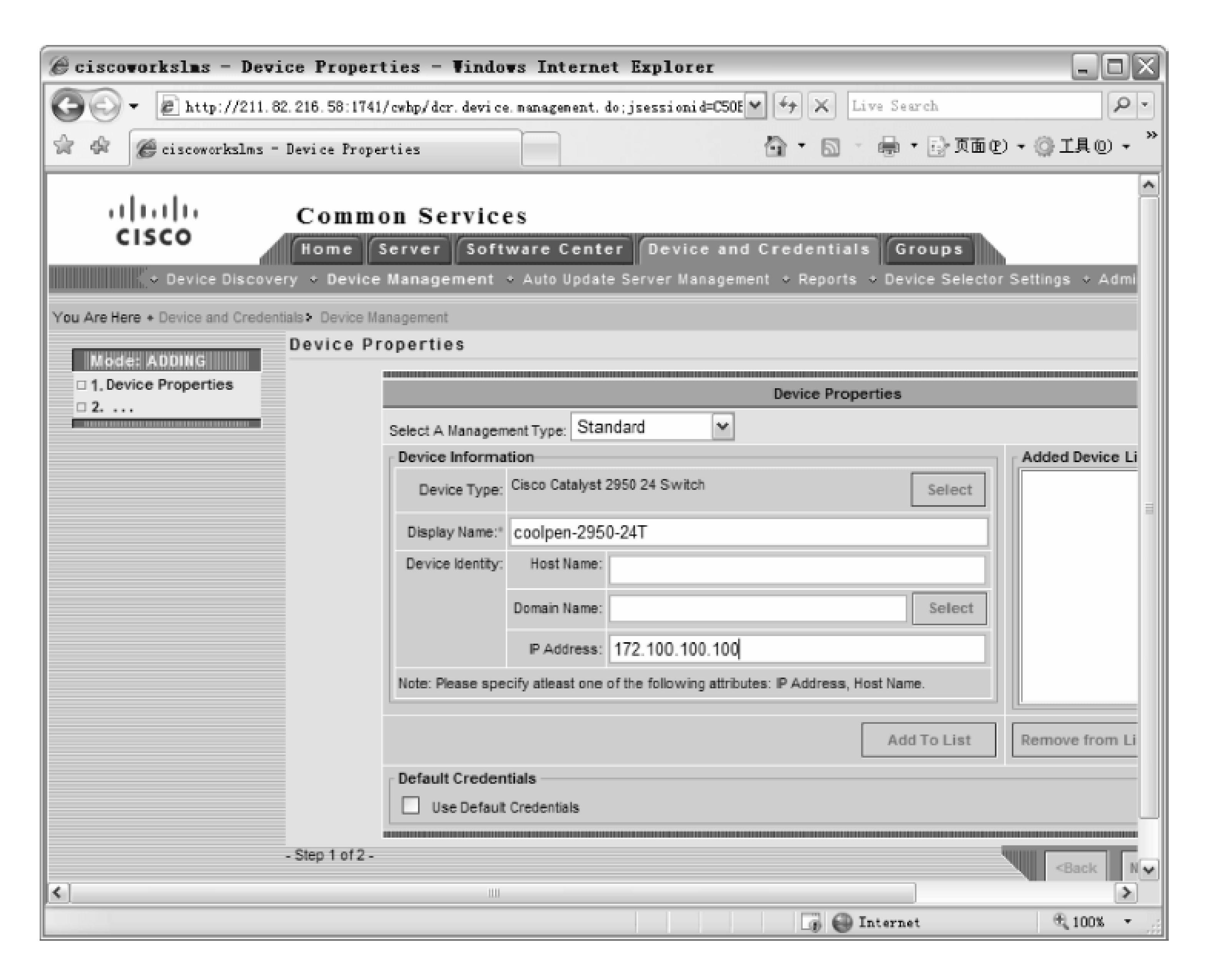


图 6-77 已选择的设备

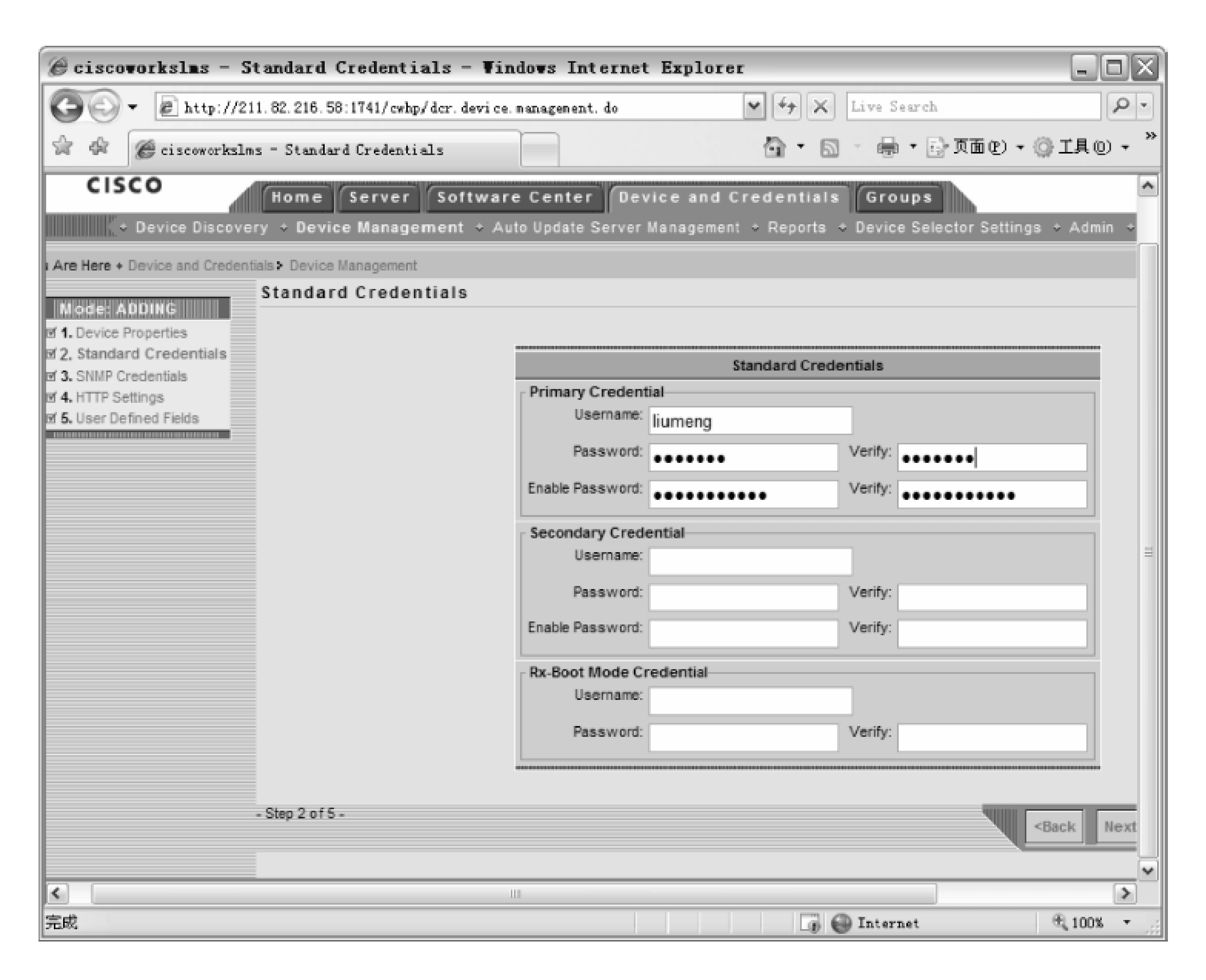


图 6-78 Standard Credentials 窗口

(6) 单击 Next 按钮,显示图 6-79 所示的 SNMP Credentials 窗口。在 RO Community String 和 Verify 文本框中,输入设备的只读字符串。在 RW Community String 和 Verify 文本框中,输入可读写的 SNMP 字符串。

(7) 单击 Next 按钮,显示图 6-80 所示的 HTTP Settings 窗口,保持默认设置即可。

(8) 单击 Next 按钮,显示图 6-81 所示的 User Defined Fields 窗口,根据需要设置用户

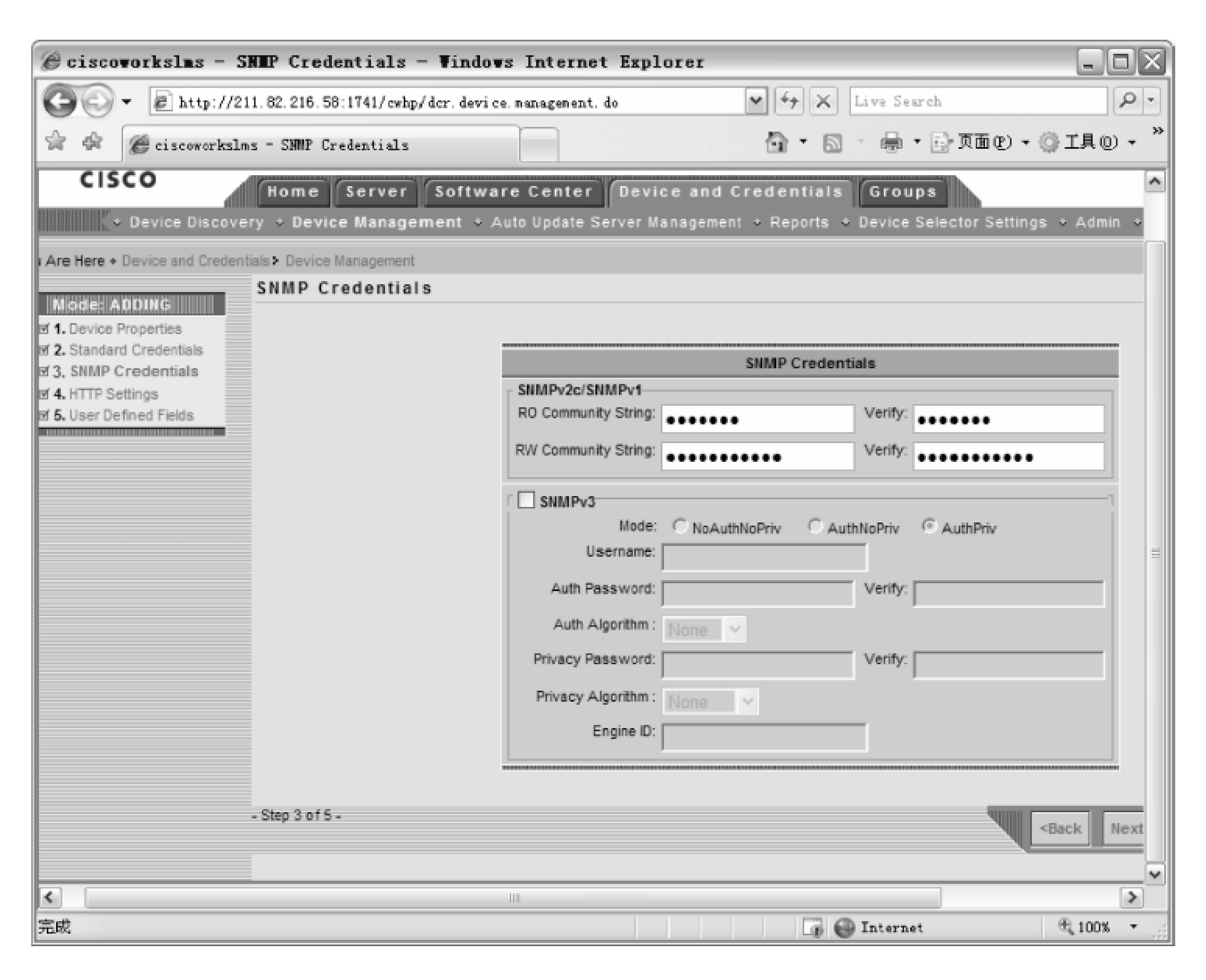


图 6-79　SNMP Credentials 窗口

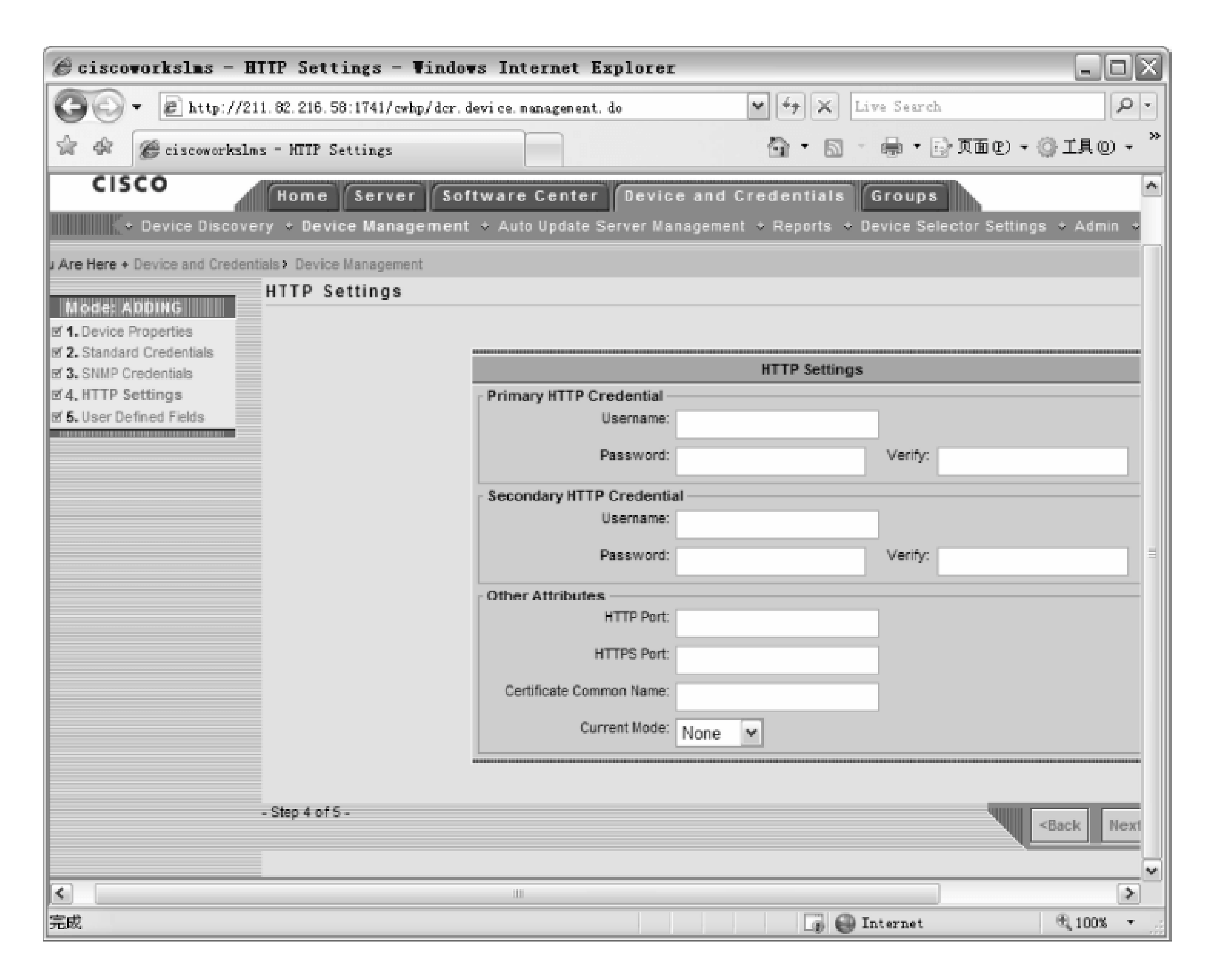


图 6-80　HTTP Settings 窗口

自定义字段,这里保持默认设置。

(9) 单击 Finish 按钮,添加成功显示图 6-82 所示的 Info 窗口。

在 Device Management 窗口中,展开 All Devices 目录,如图 6-83 所示。如果要更改某个设备的属性,可选择该设备,单击 Edit Identity 或 Edit Credentials 按钮,进行修改即可。

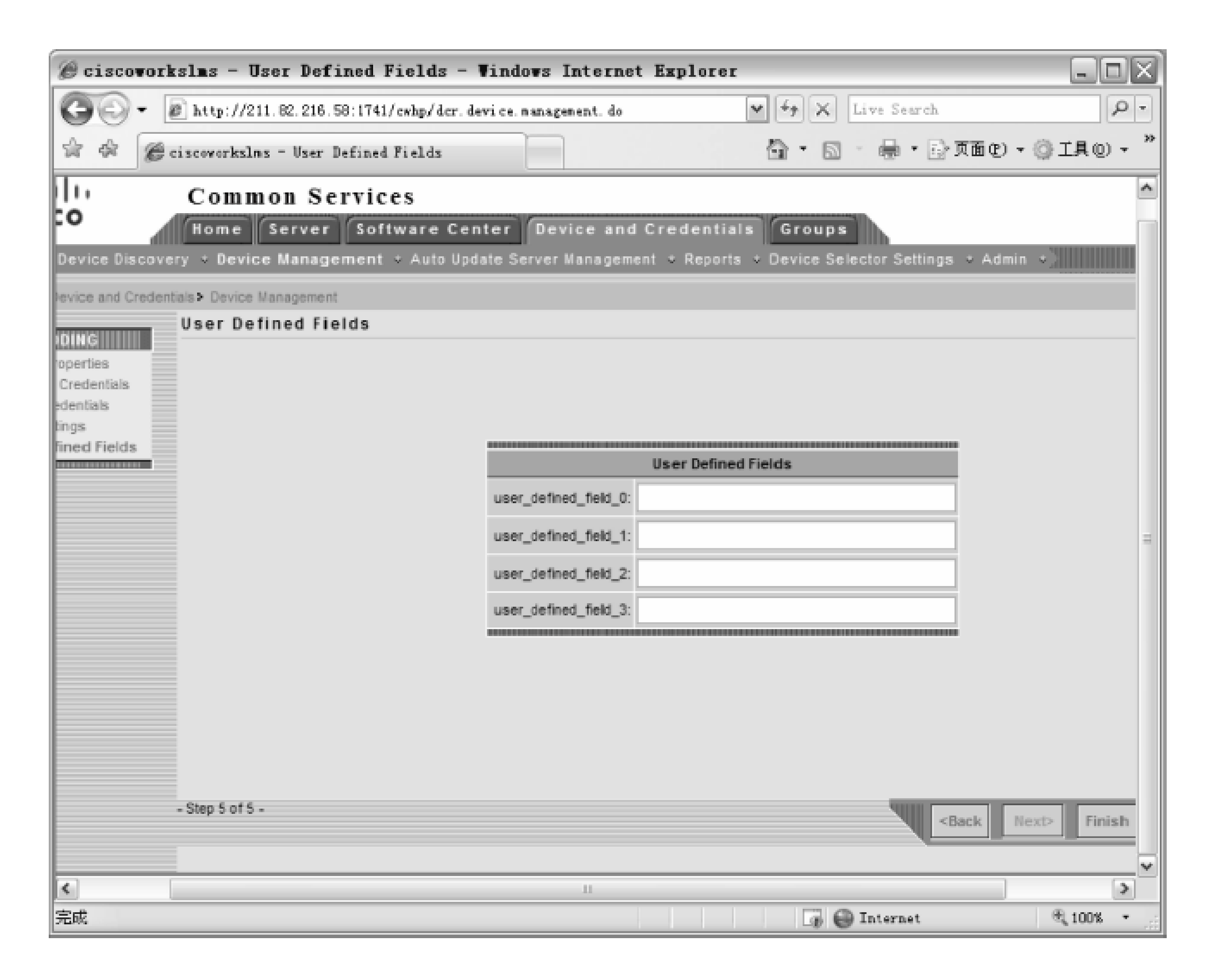


图 6-81 User Defined Fields 窗口

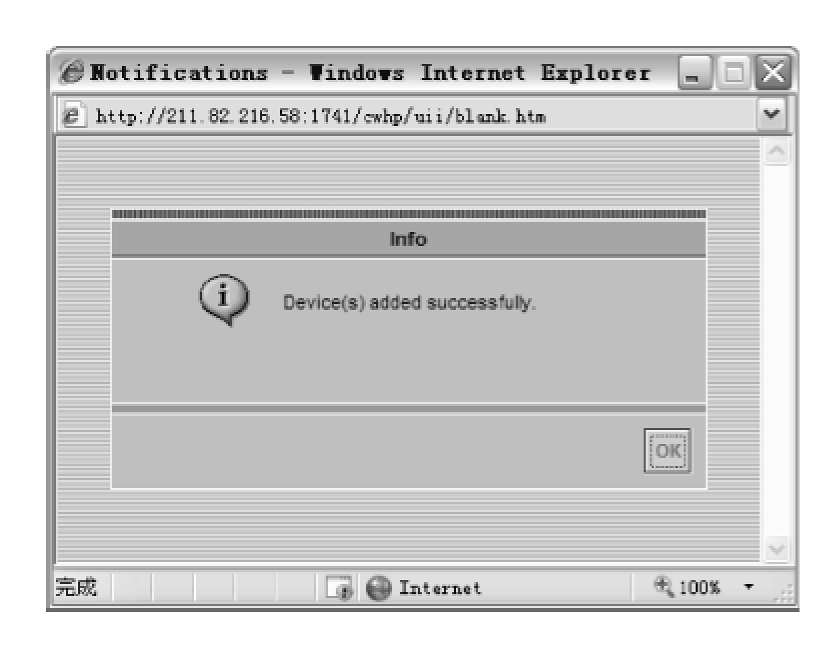


图 6-82 Info 窗口

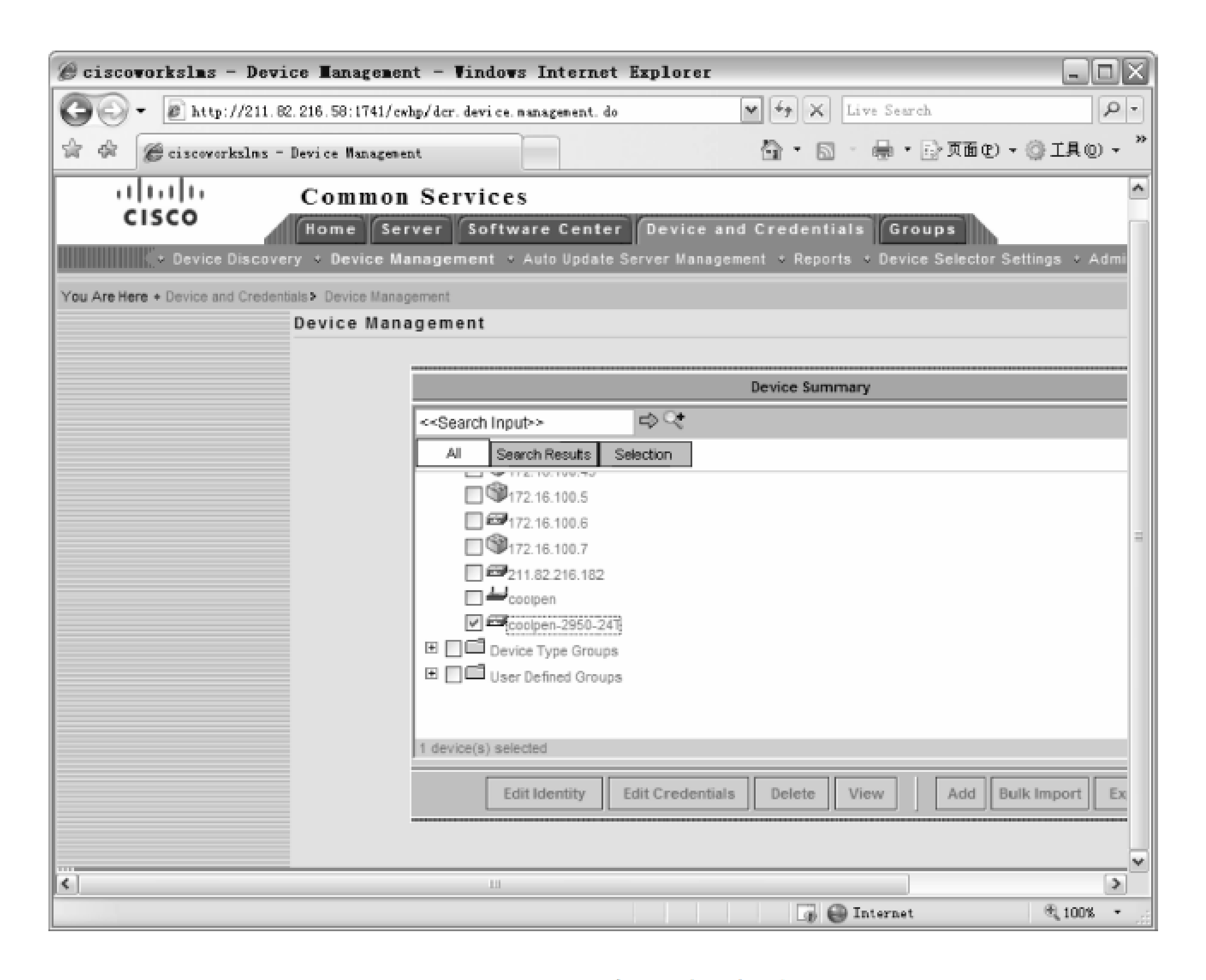


图 6-83 设备添加完成

6.6.4　在 CiscoWorks 中查看设备

设置添加完成后，即可在 Device Troubleshooting 窗口中，查看、更改、测试被管设备配置和属性。

1. 查看被管设备的属性

（1）在 Device Diagnostic Tools 窗口中单击 Device Center 链接，显示图 6-84 所示的 Device Center 窗口。

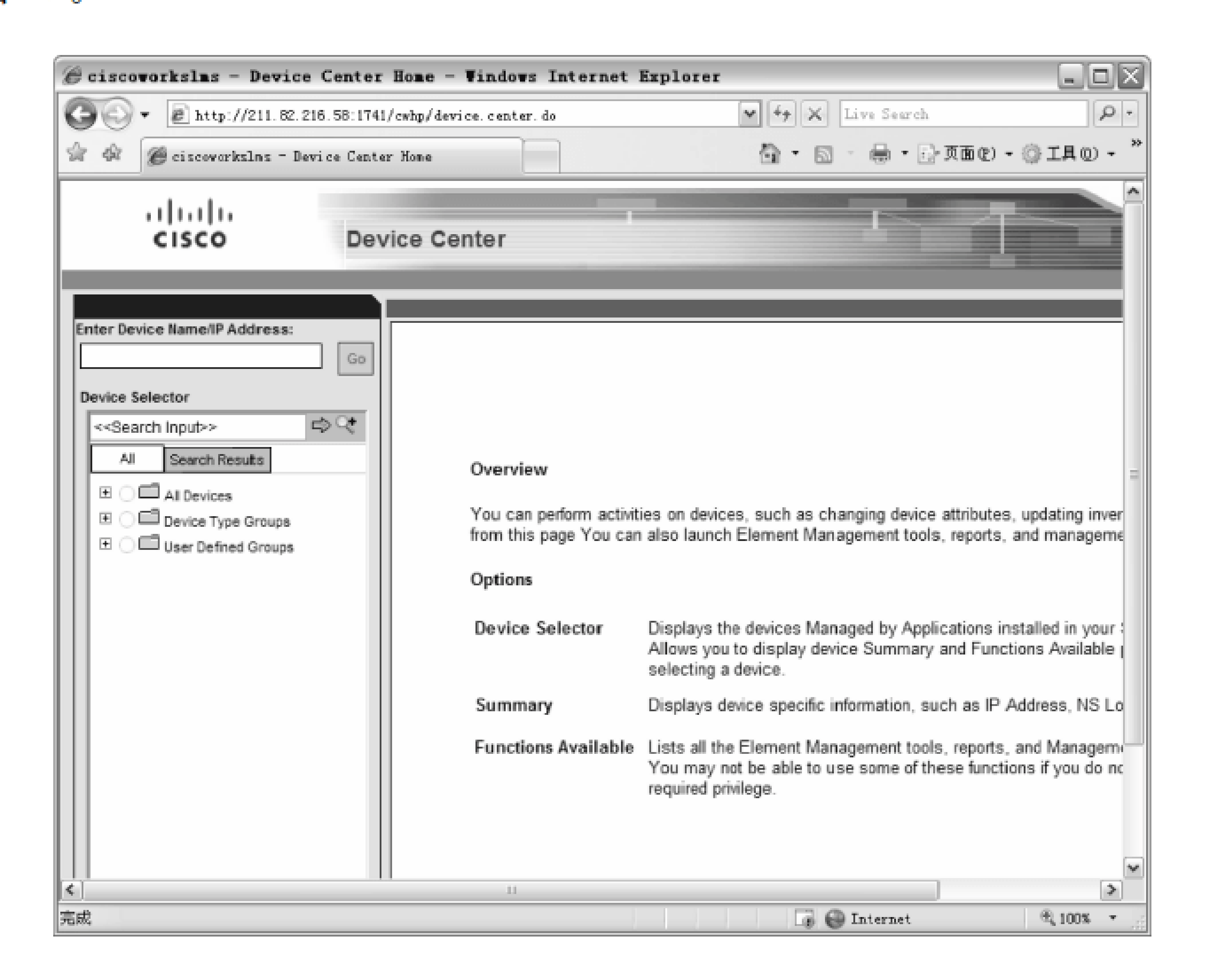


图 6-84　Device Center 窗口

（2）在 Device Selector 列表框中，单击欲查看的设备，或者在文本框中直接输入设备的名称并单击⇨按钮，即可显示设备的摘要信息，如图 6-85 所示。

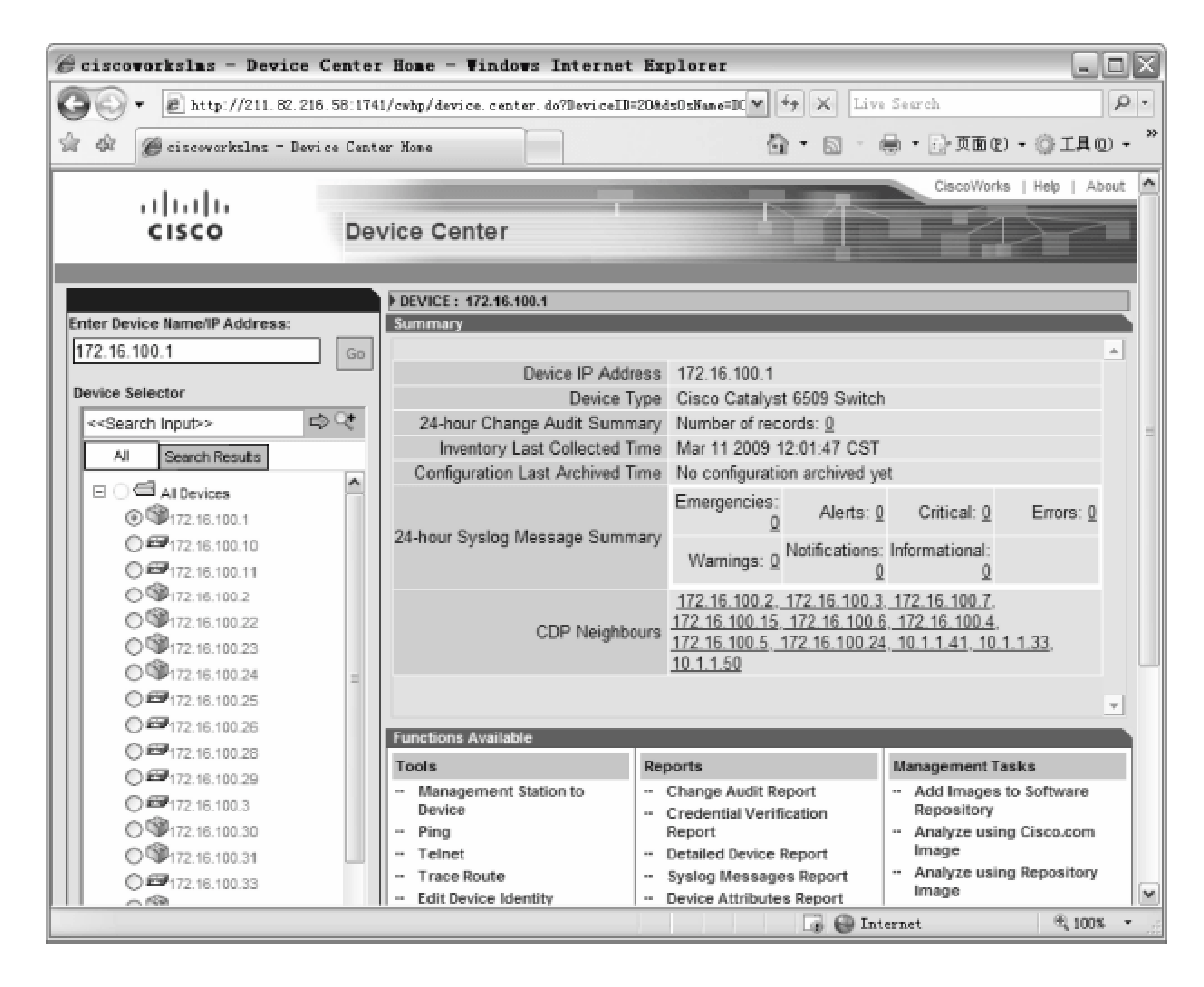


图 6-85　显示设备信息

2. 探测被管设备的被管能力

在不同的网络环境中，所使用的网络设备管理方式也有所不同，例如 Telnet、HTTP 等。通常情况下，根据不同的需要所允许的管理方式也是不相同的，使用 CiscoWorks 可以对网络设备的管理能力进行探测，测试网络中的设备可以以哪些方式登录和管理。

(1) 打开 Device Center 窗口，在 Tools 选项区域中单击 Management Station to Device 链接，显示图 6-86 所示的 Management Station to Device 窗口，选择欲测试的项目。

(2) 单击 OK 按钮，即可开始进行探测，完成后显示图 6-87 所示的 Interface Test Results 窗口，显示探测结果。如果该设备支持某种管理方式，则会显示为 Okay，如果不支持则显示为 Failed。

另外，在 Tools 选项区域中，还提供了 Ping、Trace Route 和 Telnet 等工具。而 Packet Capture 则提供了捕获设备流量的功能，可以捕获通过设备的包，但必须安装 Winpcap 软件包才能正确捕获数据包，而且还要安装 Ethereal 软件才能正确解码捕获的数据包。

3. 设置 SNMP 选项

使用 CiscoWorks LMS 还可以配置设备的 SNMP 字符串。打开 Device Center 窗口，在 Tools 选项区域中单击 SNMP Set 超链接，显示图 6-88 所示的 SNMP Set 窗口。在 Device

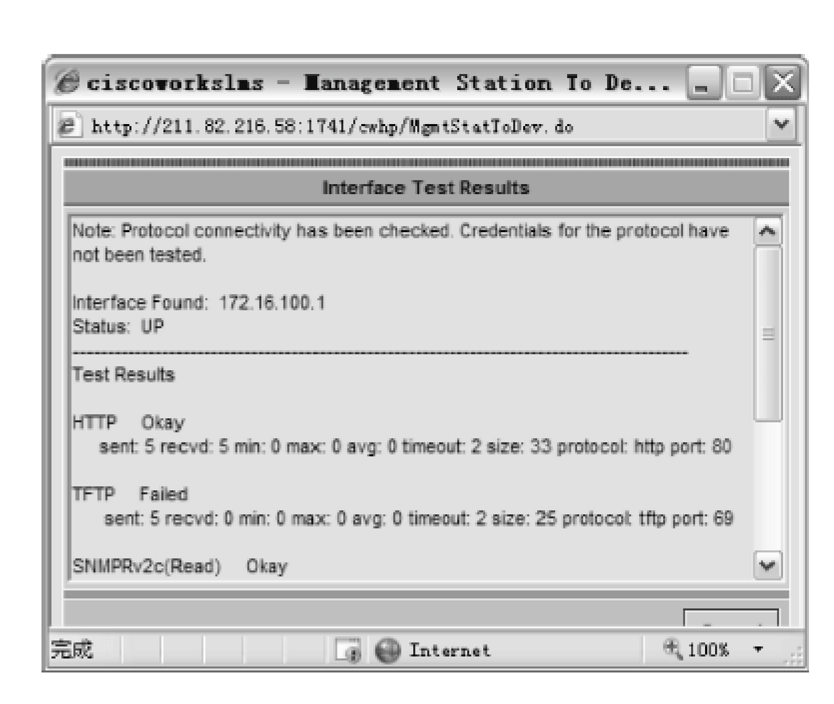


图 6-87 Interface Test Results 窗口

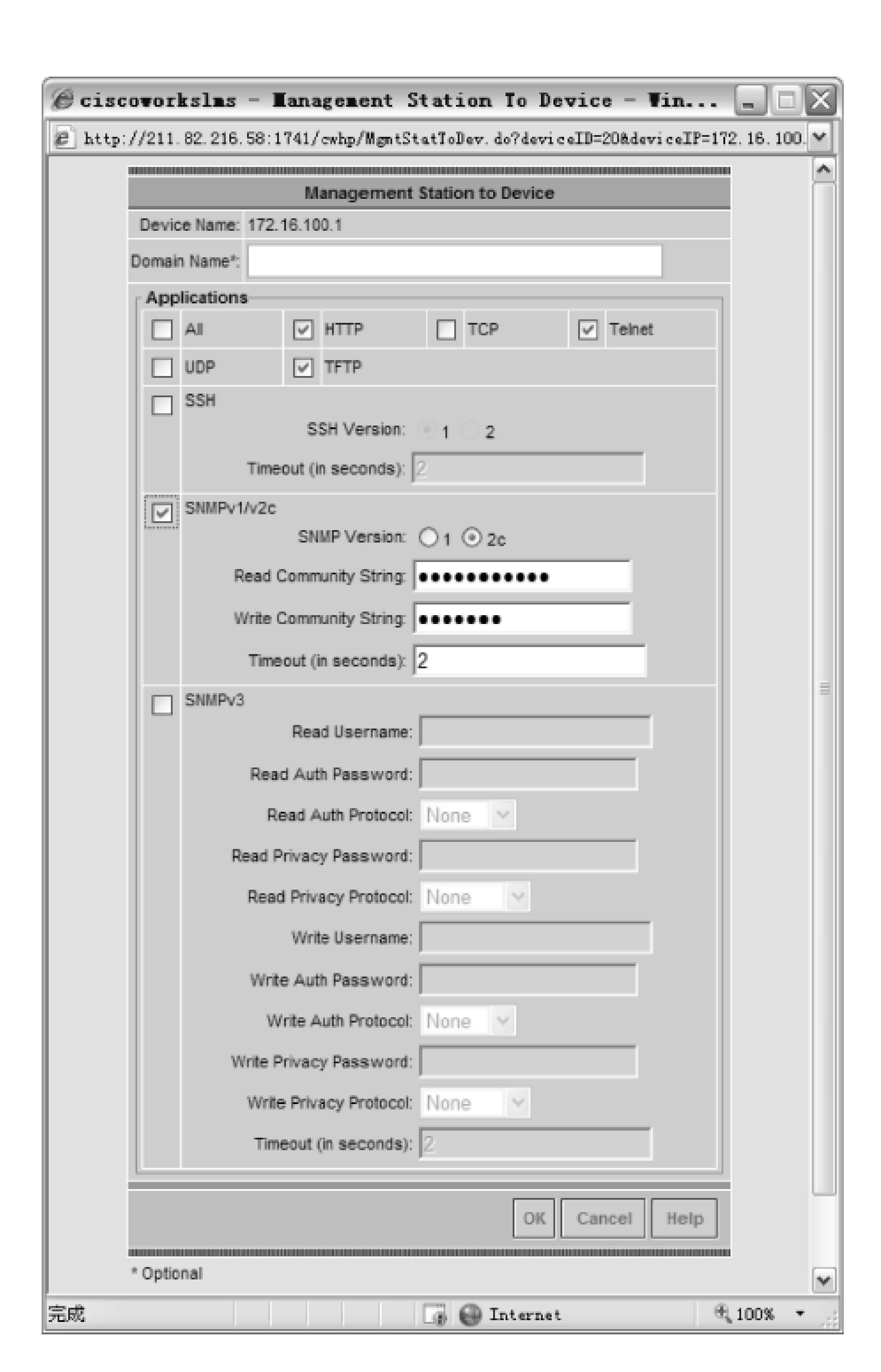


图 6-86 Management Station to Device 窗口

图 6-88 SNMP Set 窗口

Name 文本框中,输入设备的名称或 IP 地址。在 SNMP Version 选项区域中,选择所要使用的 SNMP 版本。在 RW Community String 文本框中,输入读写 SNMP 字符串。根据实际情况,设置 OID、Object Type 和 SNMP Timeout 等选项。最后,单击 Finish 按钮,确认设置即可。

4. 图形化显示设备

在 CiscoWorks 中,可以利用 CiscoView 功能以图形化的方式显示网络设备,例如实时显示设备的面板、指示灯、链路的利用率和更改设备的配置等。

(1) 在 CiscoWorks 窗口中,单击 CiscoView 窗口中的 Classis View 超链接,显示图 6-89 所示的 CiscoView(CISCOWORKSLMS)页面。

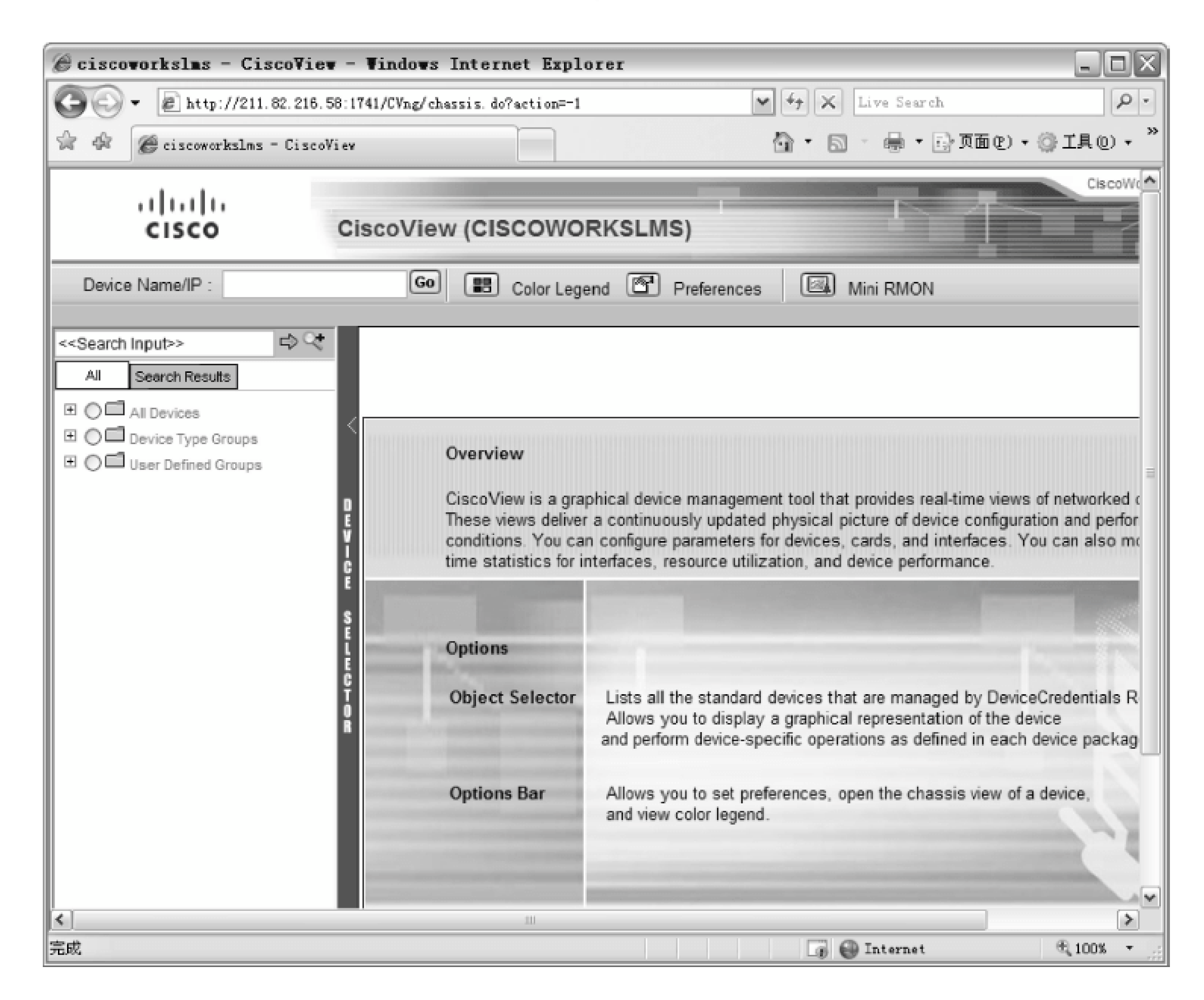


图 6-89 CiscoView 页面

(2) 在左侧列表中,选择欲查看的设备。所选设备即可以图形方式显示,图 6-90 所示为 CiscoWorks 6509 交换机的模拟图形。需要注意的是,有的交换机类型较新,某些模块可能不为 CiscoWorks 所支持,此时则会显示为 UNSUPPORTED CAID。

另外,也可以直接在 Device Name/IP 文本框中输入设备的 IP 地址,单击⇨按钮即可显示设备。不过,如果网络设置尚未添加到 CS 中,则会显示图 6-91 所示的 Please enter SNMP credentials 窗口,需要管理员提供 SNMP 口令。根据实际情况选择 SNMP 的类型,并输入 SNMP 口令,最后单击 OK 按钮即可。

6.6.5 使用 CiscoWorks 监测设备

在 CiscoView 中,还可以实时监测网络设备的使用情况。当以模拟图形显示出设备后,右击设备的非板卡区,在快捷菜单中选择 Monitor 命令,显示图 6-92 所示的设备监视窗口。

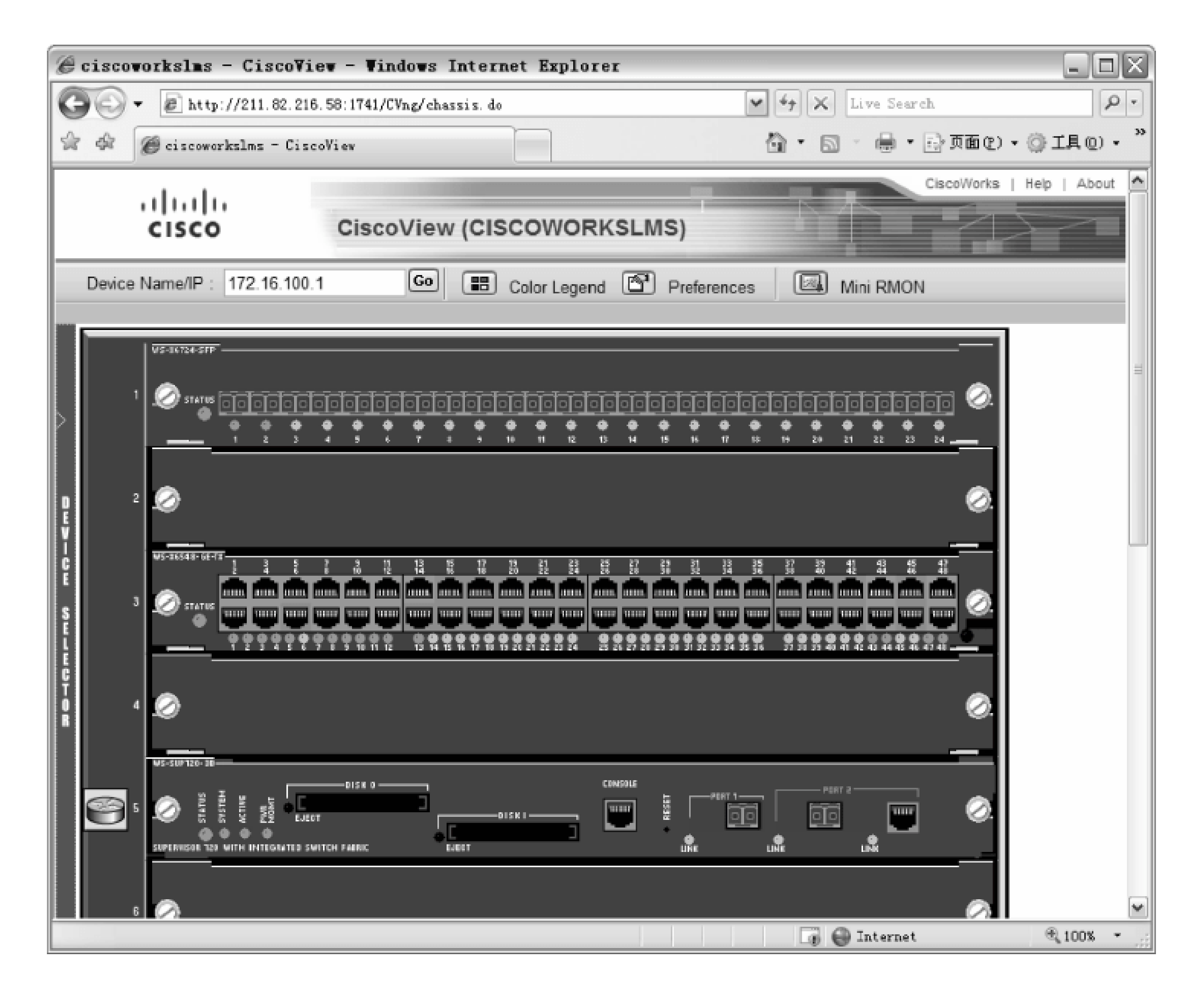


图 6-90　网络设备的模拟图形

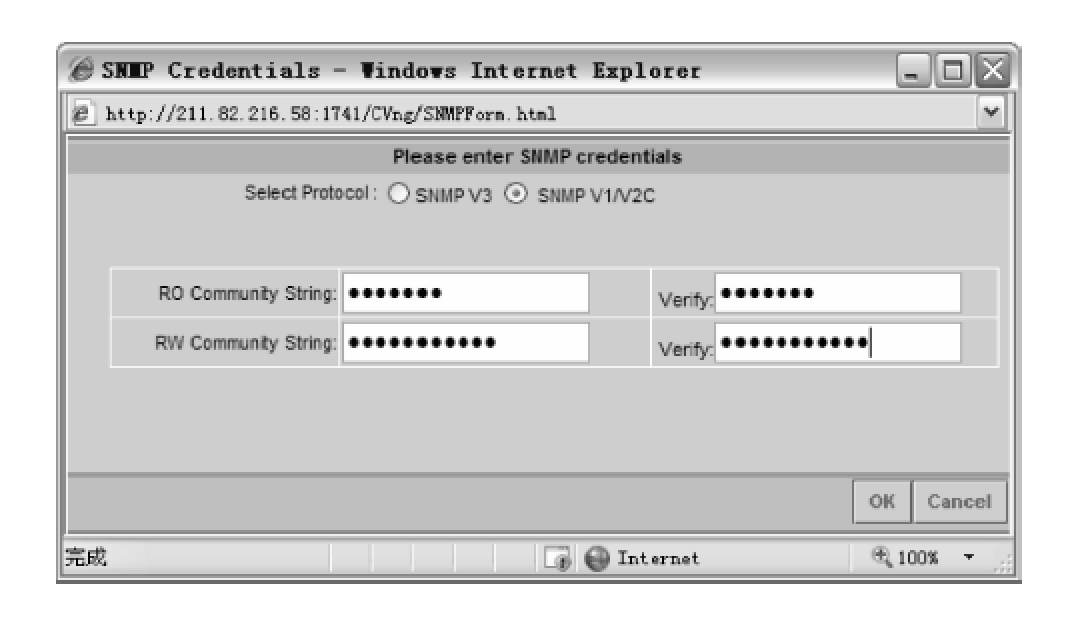


图 6-91　SNMP Credentials 窗口

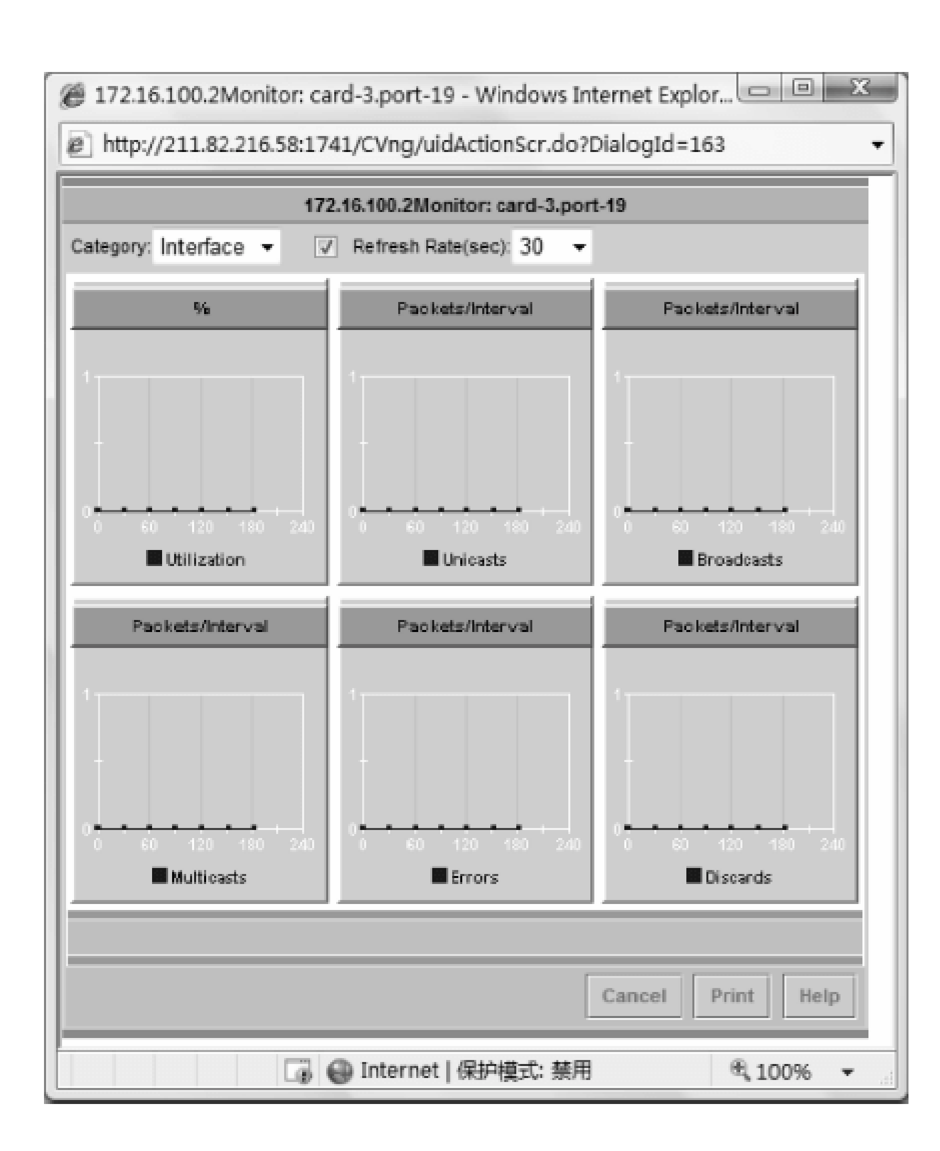


图 6-92　监视设备

6.6.6　使用 CiscoWorks 配置设备

利用 CiscoView 的配置功能，可在图形化显示设备时对设备进行简单的配置，例如设置端口的传输速率、划分 VLAN 等，使用起来非常方便。

右击被管设备模拟图形的板卡，在快捷菜单中选择 Configure 命令，即可显示配置窗口。这里选择的是交换机的端口区域，如图 6-93 所示，根据需要进行设置即可。例如，在 Name of the Port 文本框中输入端口名 1，在 Configured Speed 下拉列表框中选择 1Gbps 选

项，在 Port VLAN 文本框中输入 1，在 VLAN Port Admin Status 下拉列表框中选择端口的管理状态，如 Static。最后，单击 OK 按钮保存即可。重复操作，可继续配置其他端口。

需要注意的是，并非设备上的所有板卡都可以配置，如指示灯、电源等，只能查看而不能配置，如图 6-94 所示。

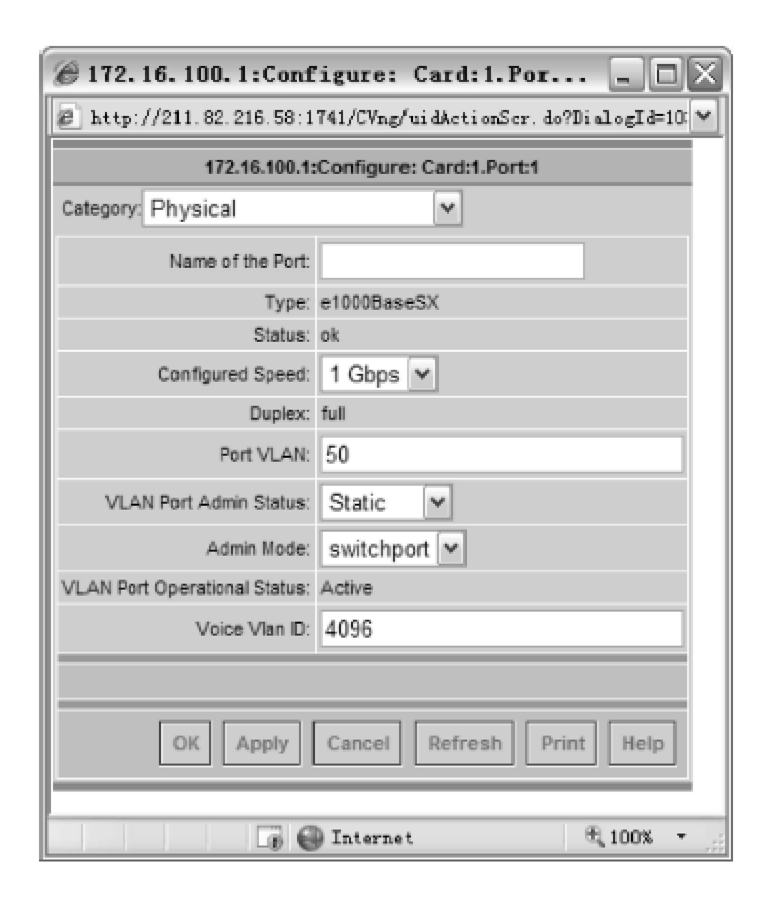


图 6-93　配置窗口

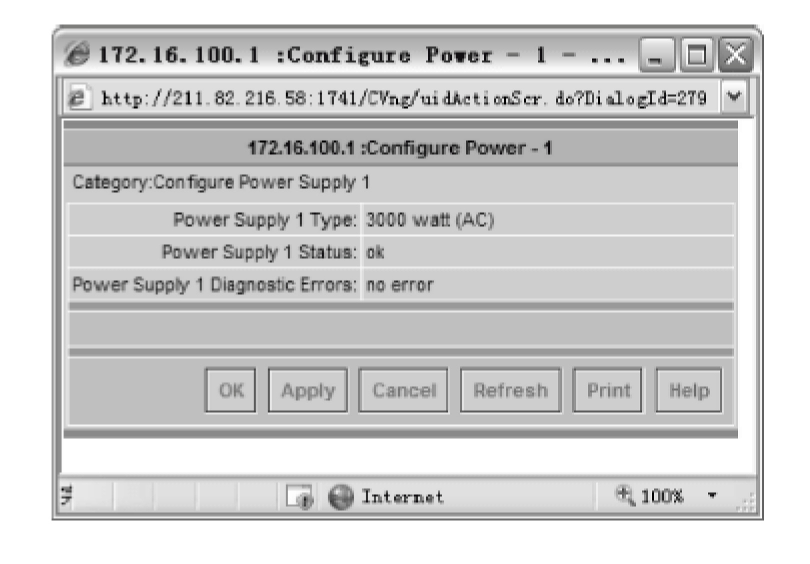


图 6-94　查看板卡配置

习题

1. 简述 Telnet 的工作过程。
2. 网络设备的初始化配置包括哪些内容？
3. 简述思科公司提供的 4 种选择 IOS 版本的方式。

实验：使用 CiscoWorks LMS

实验目的：

熟练掌握 CiscoWorks LMS 的使用方法。

实验内容：

在 CiscoWorks LMS 添加网络设备，并对网络设备进行监控。

实验步骤：

(1) 使用 CiscoWorks LMS 自动搜索网络设备。

(2) 手动添加网络设备。

(3) 查看被管设备的属性。

(4) 探测被管设备的被管能力。

(5) 图形化显示设备。

第 7 章 chapter 7

网络流量和流量监控与分析

网络每天都可能发生各种各样的问题，例如网络性能降低、数据传输不稳定等问题。甚至出现网络故障，严重影响网络的正常使用。因此，网络管理员应掌握各种网络诊断分析工具，实时地监控网络的流量和带宽等，当网络运行不畅或发生故障时，可以利用这些工具及时解决故障。

7.1 网络流量和流量监控规划

数据在网络中进行传输时，会在网络中产生流量。如果网络中的所有流量都是正常的通信数据时，通常不会有问题。但如果在网络数据中存在非法的数据，或大量的数据传输时，则有可能会造成网络故障。

7.1.1 项目背景

在当前网络中，主要的数据传输为局域网数据，即多数的计算机没有连接 Internet 的网络需求，在网络内的网络流量主要为局域网数据流量。换言之，在网络内的数据传输多为服务器与客户端之间的数据传输。

7.1.2 项目需求

网络带宽是指在一个固定的时间内能通过的最大位数据，如同高速公路的车道一样，带宽越大，好比车道越多，因此，需要清楚地了解两台计算机之间的带宽。另外，在网络中存在多个无线 AP，因为无线传输带宽的不确定性，需要进行网络带宽的测试。对于网络中的网络流量，同样需要进行相应的了解和监视，从而进行控制。而对于网络中核心设备及重要设备，则应实时进行监控，如网络吞吐量分析等。

7.1.3 解决方案

对于当前网络中网络流量和流量监控需求，可使用如下方案解决。

（1）使用以太网带宽测试（Ping Plotter Freeware）对网络质量进行测试。而对于无线网络间的带宽测试，则可以使用无线网带宽测试工具（IxChariot）完成。

（2）对网络流量的监控和分析，可以通过流量统计分析利器（CommView）和网络流量实时监控（MRTG）完成。

（3）网络吞吐量分析则可能通过 Qcheck 和 SolarWinds 完成。如果是在两个计算机之间测试，可以使用 Qcheck，如果是测试网络中的设备，则可以使用 SolarWinds。

7.2 网络带宽监控与分析

影响网络带宽的因素主要是网络线路，通常情况下，在网络建设完成之初，因为设计的原因，网络带宽都会满足网络的需求。但随着网络使用时间的不断增长，因为线路老化或干扰等原因，可能会对网络带宽产生影响。因此，需要使用网络带宽测试工具测试网络带宽，以时刻掌握网络带宽的具体情况。

7.2.1 以太网带宽测试——PingPlotter Pro

PingPlotter 是一款多线性的跟踪路由程序，能最快地显示当前网络出现的问题。PingPlotter 的功能类似于 Windows 中的 Tracert 命令，但与其所不同的是，该工具具有信息同时反馈的速度优势，并且 PingPlotter 不仅可以以数据方式显示，还可以以图形方式显示。与其他检测分析工具相比，检测分析结果更为直观和易于理解。PingPlotter 可从其官方网站下载，地址为：http://www.pingplotter.com/，分为标准版和专业版两种，可运行于 Windows 9x/NT/2000/XP/2003/Vista/2008 等操作系统，这里以 PingPlotter Pro 为例。

PingPlotter Pro 下载并安装完成以后运行，显示图 7-1 所示的 PingPlotter Pro 窗口。在 Address to Trace 文本框中，输入要追踪路由的域名或 IP 地址；在＃ of times to trace 文本框中，设置追踪时间，默认为 Unlimited，表示一直追踪下去；在 Trace Interval 文本框中，设置追踪的间隔时间，默认为 15seconds；在 Samples to include 文本框中，设置采样数量，默认是 10 个。

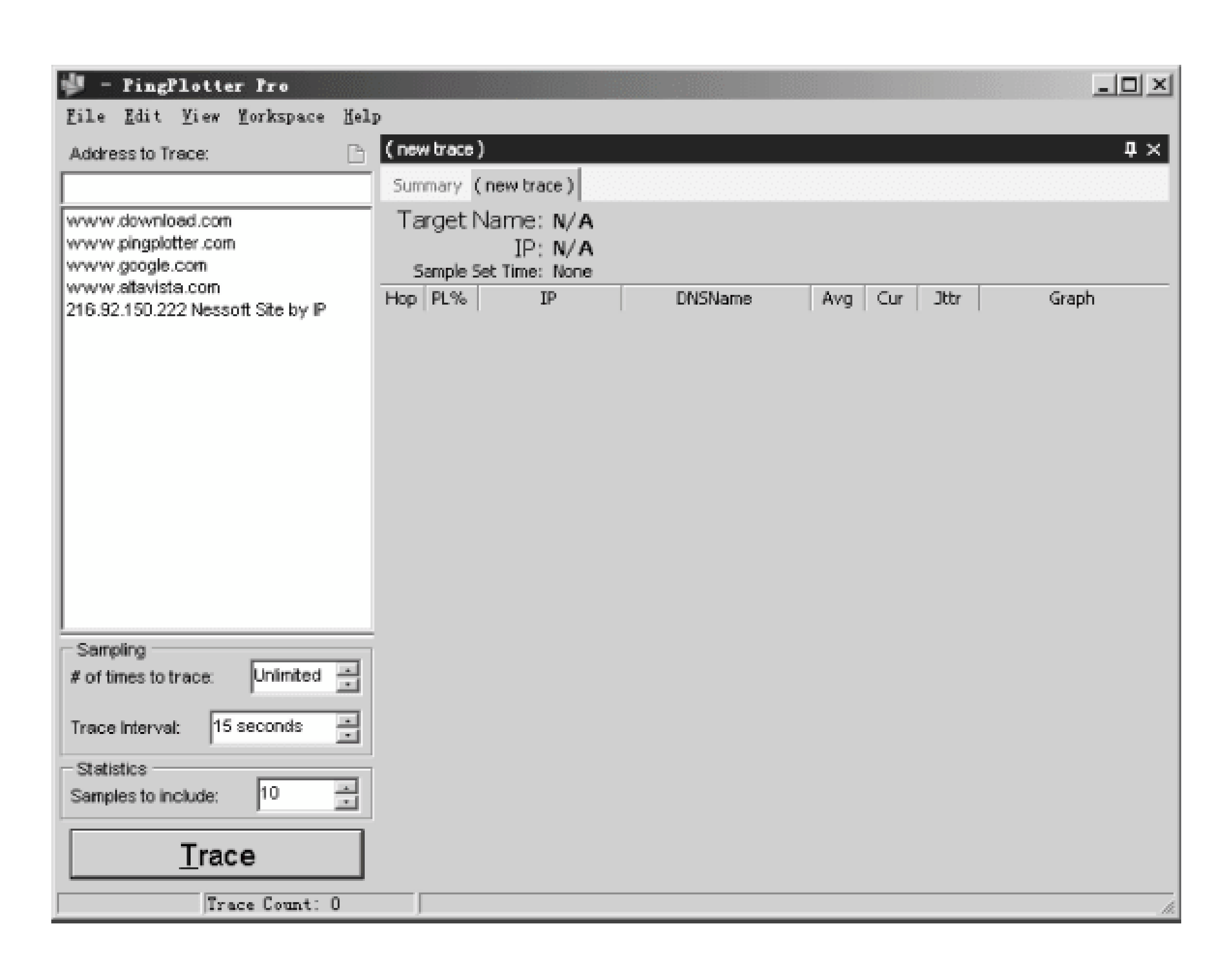


图 7-1 PingPlotter Pro 窗口

这里以查看追踪到百度网站时所经过的路由为例。在 Address to Trace 文本框中输入网址：www.baidu.com，单击 Trace 按钮，PingPlotter Pro 即可开始追踪百度网站，并在窗

口右侧显示 www.baidu.com 的图形表，如图 7-2 所示。从表中可以查看所追踪网址的名称和解析出来的 IP 地址，在中间的节点列表中，显示了从本地计算机到目标主机所经过的 IP 地址、DNS 域名、此主机的平均响应时间（Avg）、到目标主机丢失的数据包数，通过该曲线图就可以看出网络出现的问题。

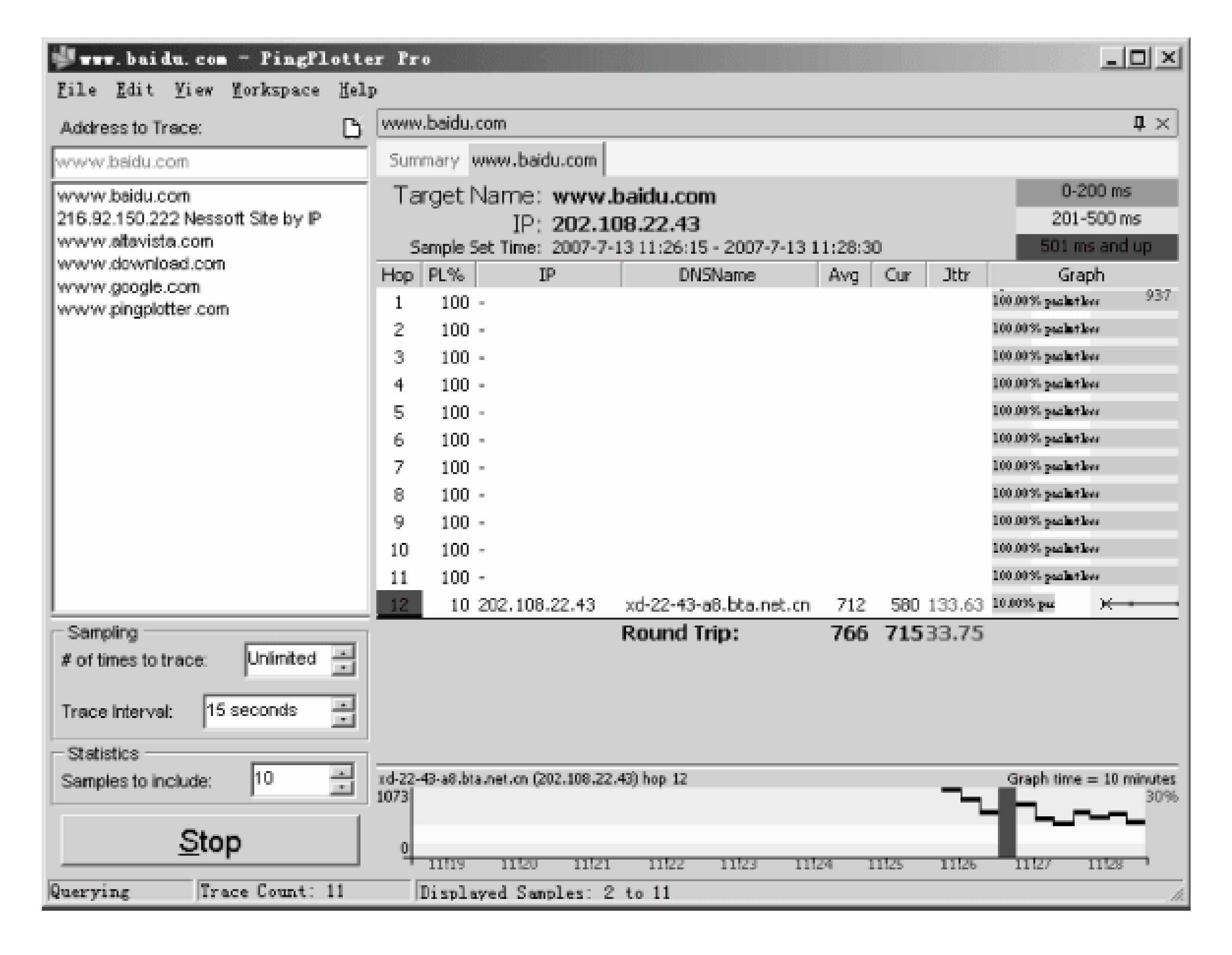


图 7-2 测试结果

在追踪路由时，会以不同的颜色显示所经过的路由的状态，在窗口右上角显示了不同颜色代表的不同响应时间，例如，在该图中，经过的路由以红色显示，表示该路由处于堵塞状态，以致发到目标主机的数据包在这里丢包严重，影响了数据的传递。如果显示为绿色，则表示速度良好。

提示：在测试时，应多连接一些国内外的各大网站以进行比较，从而知道自己的网络状况到底如何。

在使用 PingPlotter 测试时，可以将当前的测试结果以图形或文本的形式保存起来，以便日后比较查看。依次选择 File→Save Image 命令，即可将当前测试结果保存成图片文件，选择 Export to Text File 命令则可将测试结果输出到文本文件。

在 Edit 菜单中，选择 Copy as Image 或 Copy as Text 命令，分别可以把当前窗口的图形格式或文本格式复制到剪贴板中。选择 Options 命令，则显示图 7-3 所示的 Options 对话框，可以对 PingPlotter 进行设置，如显示方式、保存方式和更改路由等。

小知识：PingPlotter 与 Tracert 命令相比，界面直观且信息反馈速度更快。通过利用国内外一些大网站进行测试，可以综合地评价一家运营商的宽带网络质量，中间所经过的节点越少越好，然后结合其他指标，即可比较出哪一家运营商的宽带接入质量比较好。

7.2.2 无线网带宽测试工具——IxChariot

由于具有灵活性、使用简单等特点，无线网络被广泛应用于许多家庭、小型办公室、酒店及一些不易布线的场所。而周围存在各种电磁波会干扰无线网络的传输，为了了解无线网络的带宽情况，需要使用一些专用的无线网络测试工具，例如 IxChariot 就可以帮助用户测试出网络带宽。

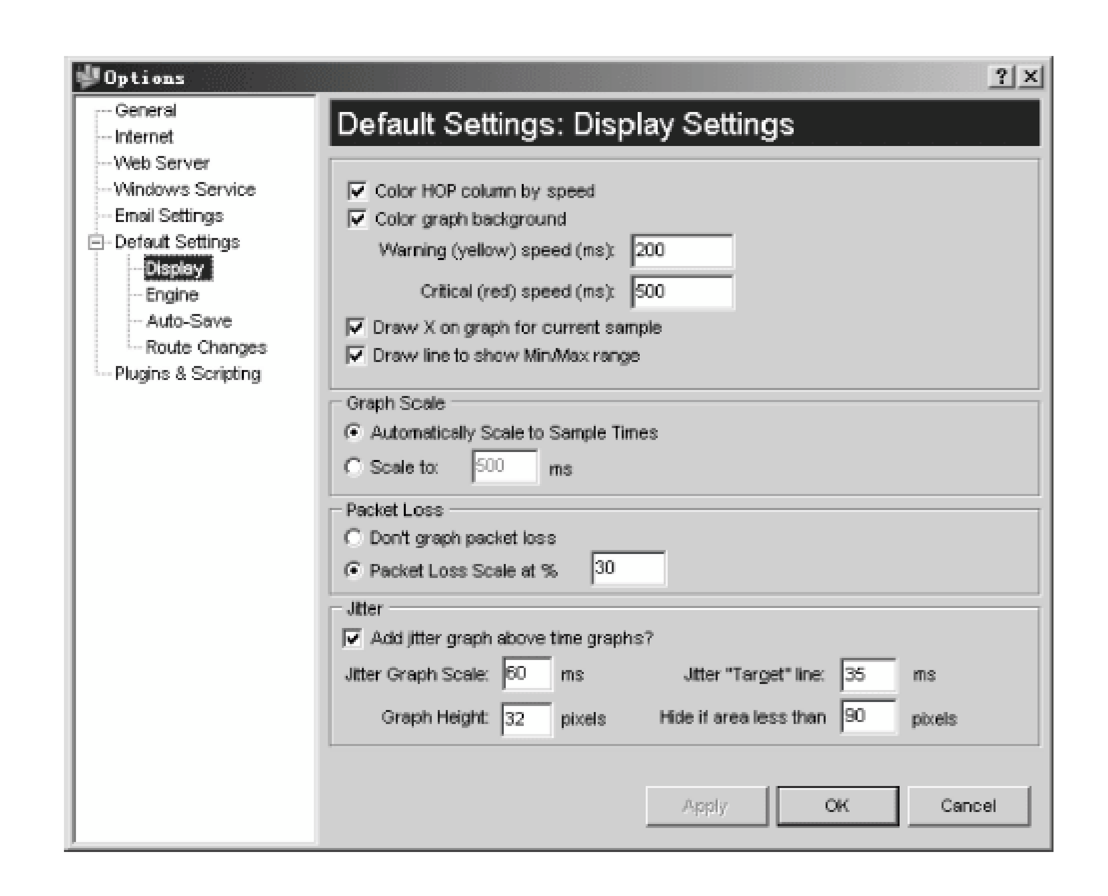


图 7-3 Options 对话框

1. IxChariot 概述

IxChariot 是美国 NetIQ 公司推出的一款网络测试软件,可以在各种网络环境下测量两台计算机之间的连通带宽。IxChariot 通过主动式定量的测试方式,产生真实的流量,测试网络设备或网络系统在真实应用时端到端的性能。IxChariot 可广泛适用于 IP 网络及网络设备应用层性能测试,比如 VOIP、IPv6、故障检测、QoS、GPRS 的 IP 应用测试等。

IxChariot 附带各种测试脚本,可以测试网络中的数据流量、响应时间以及数据吞吐量等信息。IxChariot 的测试脚本可以分为 Internet Scripts、Benchmark Scripts、Business Scripts、Streaming Scripts 等几大类,而在每一类测试中又针对不同的应用而设置了相应的脚本,例如,公司欲进行视频会议,就可以通过 Streaming Scripts 中的 NetMeeting Scripts 测试网络性能;而对于邮件系统则可以使用 Lotus Notes 或 cc:Mail Script。

2. 测量无线网的单向网速

这里以测量无线网络中的两台计算机之间的带宽为例进行介绍,这两台计算机的 IP 地址分别为 192.168.1.6 和 192.168.1.8。

首先,需要在这两台计算机上均安装 IxChariot;另外,为了得到更准确的值,建议在测试的两台计算机上均关闭防火墙,并关闭正在运行的其他程序。

(1) 依次选择"开始"→"程序"→IxChariot→IxChariot Console 命令,运行 IxChariot 程序,显示图 7-4 所示的 IxChariot 窗口。在 IxChariot 窗口左侧有 4 个按钮:单击 New 按钮可新建一个测试;单击 Open 按钮可打开以前保存过的测试文件;单击 Design 按钮则可查看各种按钮的使用说明;单击 Help 按钮提供帮助。

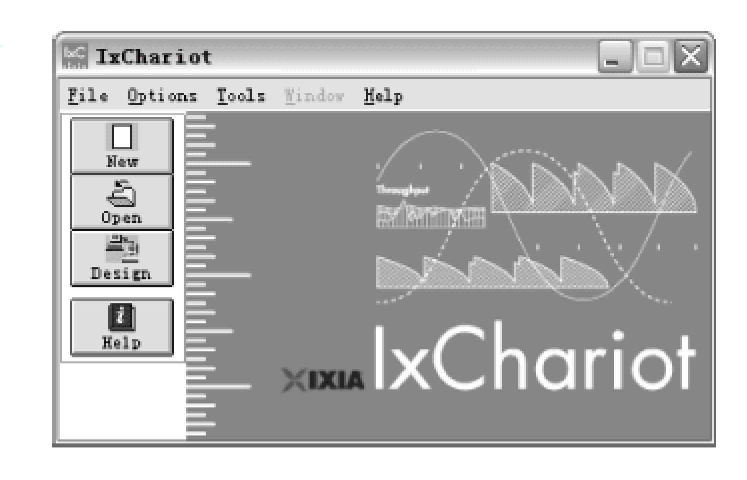


图 7-4 IxChariot 主窗口

(2) 单击 New 按钮,显示图 7-5 所示的 IxChariot Test 窗口,在该窗口中可创建新端点并进行测试。

(3) 由于是要测试两点之间的吞吐量,因此,单击工具栏上的[图标]按钮,显示图 7-6 所示的 Add an Endpoint Pair 对话框。在 Pair comment 文本框中,输入测试名称;在 Endpoint 1 to Endpoint 2 选项区域中,分别输入两台计算机的 IP 地址;在 Network protocol 下拉列表框中选择所使用的协议,默认使用 TCP 协议即可。

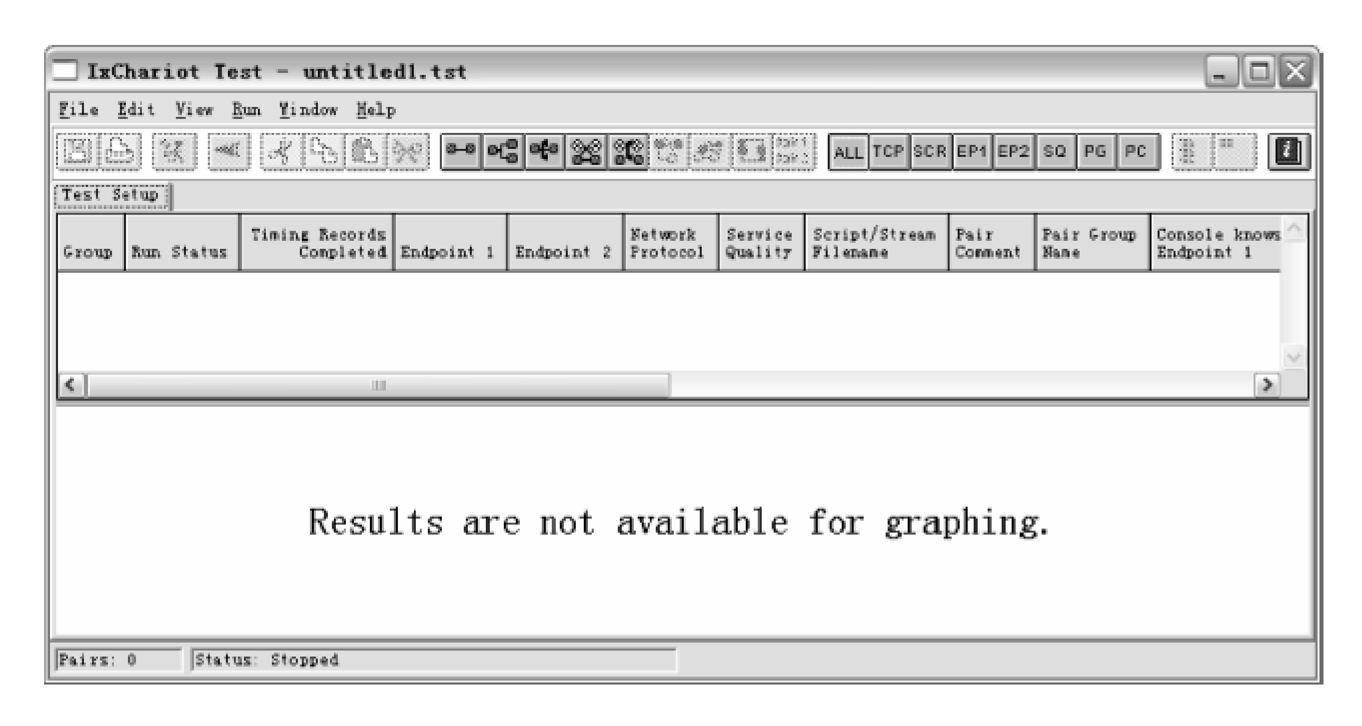


图 7-5 IxChariot Test

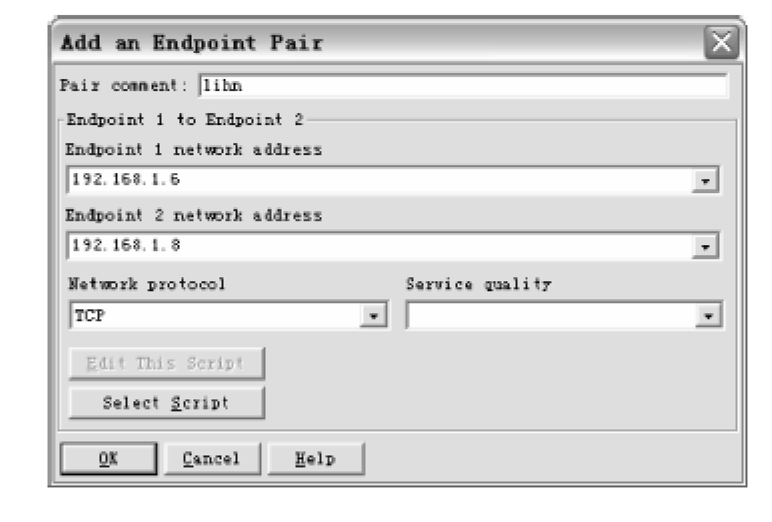


图 7-6 Add an Endpoint Pair 对话框

(4) 单击 Select Script 按钮,显示图 7-7 所示的 Open a Script File 对话框,选择一个测试脚本。测试两点间的带宽,也就是通过测试两点之间的吞吐量来得出带宽值,因此,选择 IxChariot 自带的 Throughput 脚本即可。

(5) 单击 Open 按钮,返回 Add an Endpoint Pair 对话框,单击 OK 按钮,完成新测试的创建,并添加到 IxChariot Test 窗口的 Test Setup 列表框中。重复操作,可创建多个测试。

(6) 单击按钮,IxChariot 即可开始测试两台计算机间的带宽。此时,在 Throughput 区域以图表方式列出了不同时间段的数据包发送时的值,如图 7-8 所示。

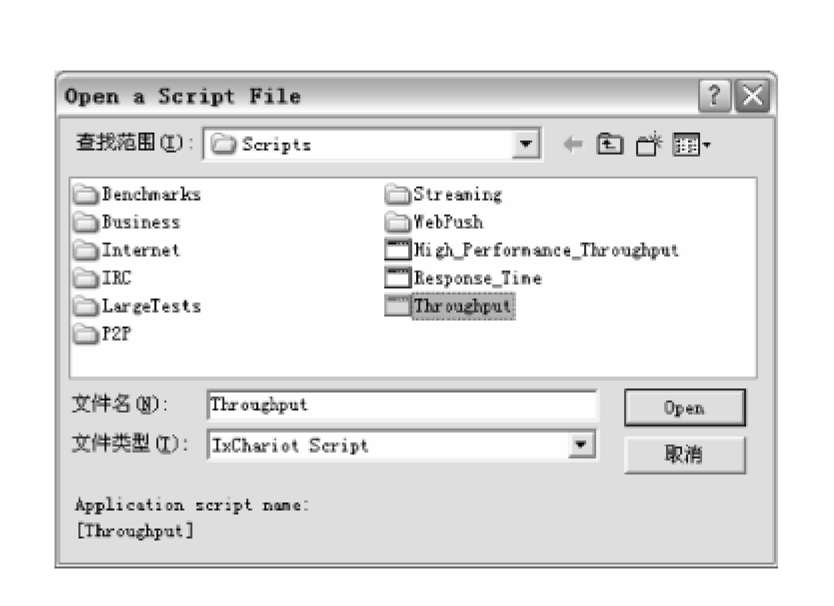


图 7-7 Open a Script File 对话框

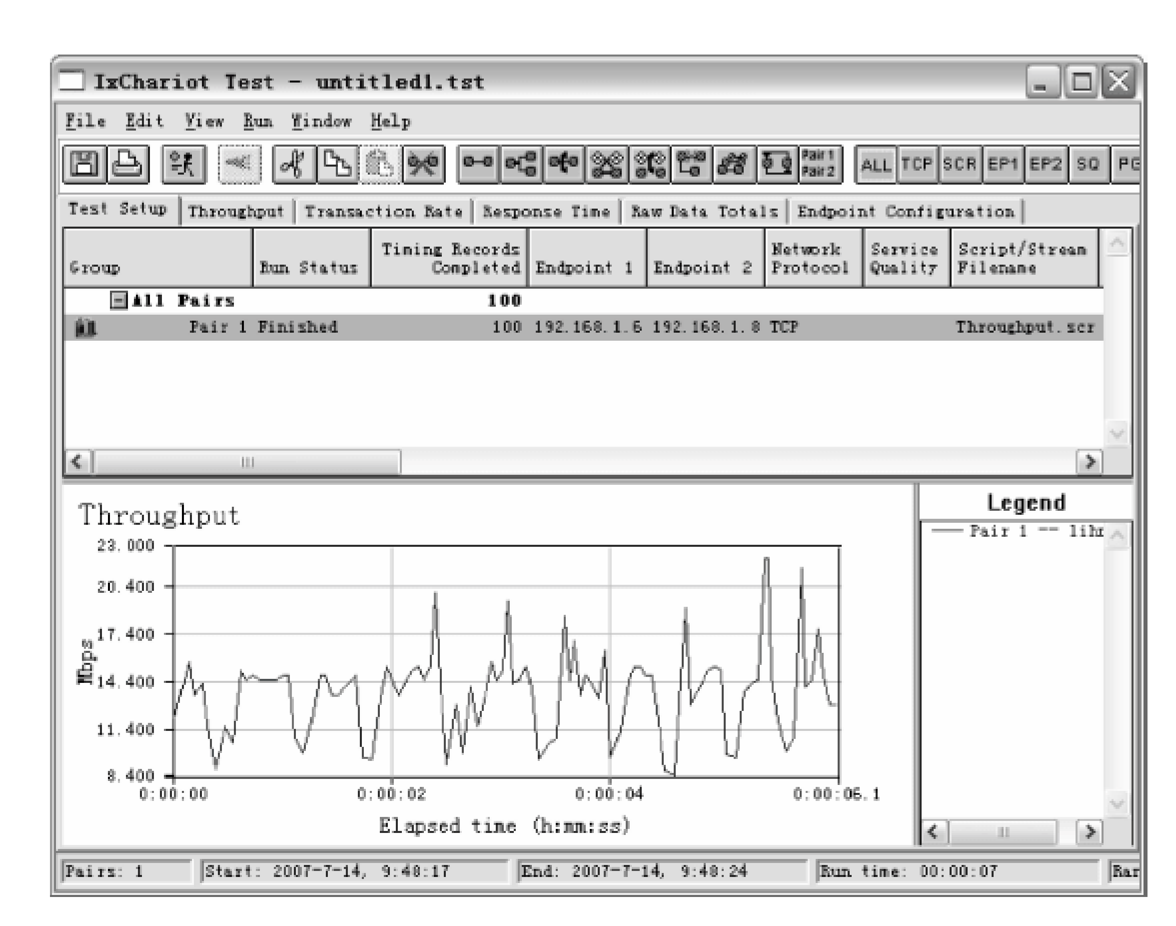


图 7-8 测试结果

注意:在测试时,必须将 IxChariot 窗口拉伸到足够大,如果窗口太小则不能显示图形界面,并会提示 This region is too small to show a graph. Maximize or resize this application,此时只要将窗口最大化即可。

(7) 选择 Throughput 选项卡,在该窗口中显示了测试时的详细数值,如 Average(平均值)、Minimum(最小值)和 Maximun(最大值)等,如图 7-9 所示。IxChariot 通过测试 100 个数据包从一台计算机发送到另一台计算机所使用的速率,计算平均值,来得出两点之间的带宽。需要注意的是,由于无线带宽的损耗,往往测量得到的真实带宽要比标称值小一些。

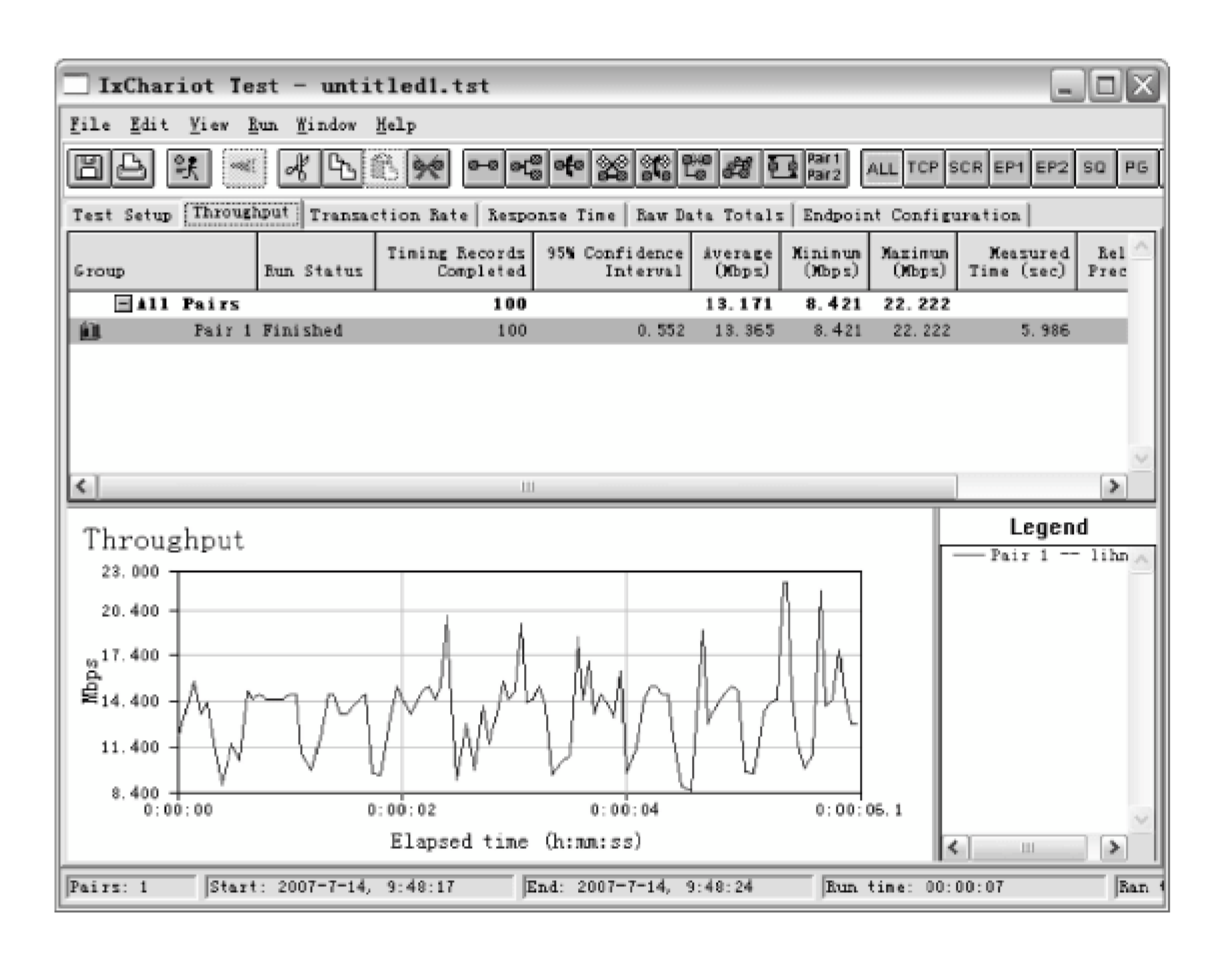


图 7-9 Throughput 选项卡

注意：IxChariot 通过统计一个预定长度和格式的脚本文件无差错地从一台服务器传送到另一台服务器的时间来计算出路由器的吞吐量，因此，计算机性能的好坏也影响着测试值。

3. 测量无线网双工方式时的网速

由于单双工模式因为自身设计的原因，会严重影响网速，所以目前几乎所有的网卡和集线设备均支持全双工模式。对网络带宽的测试，不能仅仅局限于从一台计算机到另一台计算机的网络带宽。所以在使用 IxChariot 进行测试时，尽量使用全双工模式进行测试。

（1）在一台测试机上运行 IxChariot 程序，单击 IxChariot 窗口中的 New 按钮，打开 IxChariot Test 窗口。

（2）依次选择 Edit→Add Pair 命令，创建一个新测试。在 Endpoint 1 network address 文本框中，输入 IP 地址 192.168.1.6；在 Endpoint 2 network address 文本框中，输入 IP 地址 192.168.1.8；然后单击 Select Script 按钮选择 Throughput 脚本。

（3）由于要求测量网络双向吞吐量，所以还需要再添加一个反向的测试。单击 Add Pair 按钮再创建一个测试，在 Endpoint 1 to network address 文本框中，输入 IP 地址 192.168.1.8；在 Endpoint 2 to network address 文本框中，输入 IP 地址 192.168.1.6，单击 Select Script 按钮选择 Throughput 脚本，如图 7-10 所示。

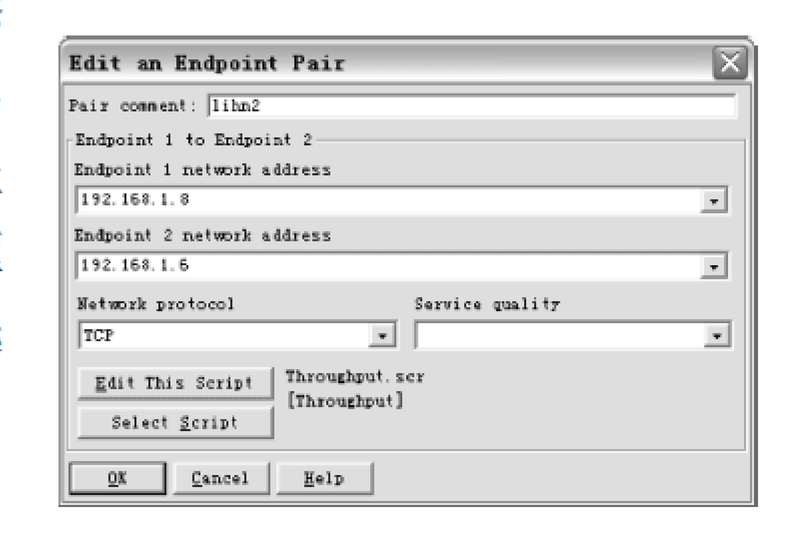


图 7-10 建立双向测试

（4）单击 OK 按钮，完成两个测试的添加。

（5）单击 Run 按钮即可开始测试，测试完成以后，在图表中不同颜色的曲线代表不同的测试点，如图 7-11 所示。

（6）测试完成后选择 Throughout 选项卡，即可查看具体测量的带宽值，如平均值、最小值和最大值等，如图 7-12 所示。通过查看这些数据，可以了解网络带宽的质量。另外，为了求得更精确的值，建议多测试几次。

在测试无线带宽的同时，也能测试无线路由器的性能优劣。如果路由器本身性能较差，

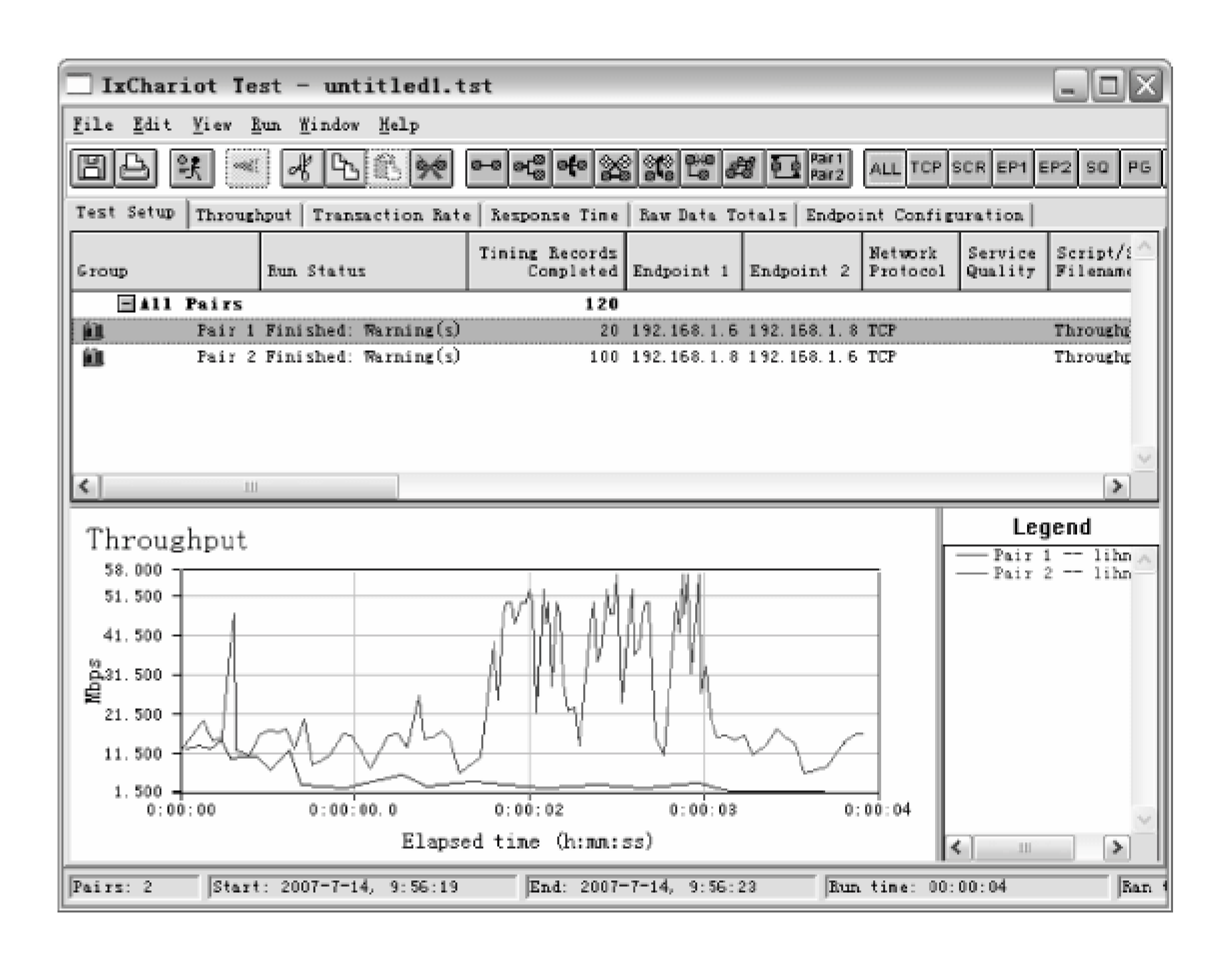


图 7-11 开始测试

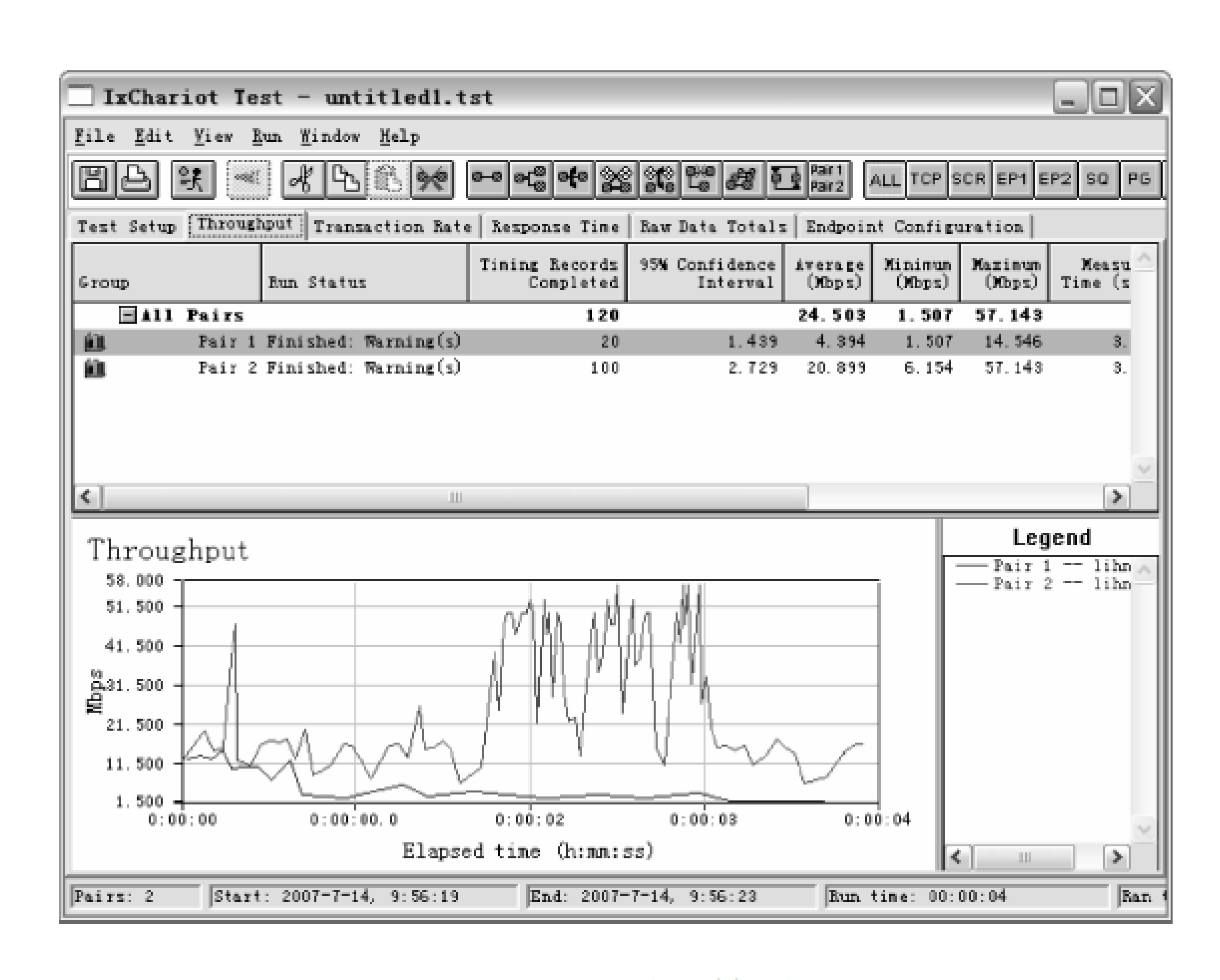


图 7-12 测量结果

在只有一对连接时测试所得出来的数据，虽然测试值可能会比较高，但并不代表无线路由器性能也高。因此，测试时应使无线路由器多连接一些计算机，只有在多连接的情况下还能得出较高的测试值时，才说明该无线路由器性能比较好。

4. 提高测量准确性

因为网络每时每刻都在发生着变化，因此每次所测量得到的结果是不相同的。通常情况下，为了使测量结果更加接近于真实数值，需要进行多次测量，从而得到多次测量的平均值。

(1) 多对 Pair 测量法

多对 Pair 测量法，是将创建的一对 Pair 复制多份，使 IxChariot 同时测量所有的 Pair。这种方式一般用来测试网络不稳定、经常出现速度波动的情况。通过采用平均值，将所有测量值汇总在一起即可得到更接近真实数值的结果。使用多对测量的方法在一定程度可减少误差，使得测量结果更加准确。

① 打开 IxChariot 程序，在 IxChariot Test 窗口中，单击 Add an Endpoint Pair 按钮，创建一个 Pair，并根据需要选择 Throughput 脚本。

② 创建完成以后，在 IxChariot Test 窗口中右击新建的 Pair，在快捷菜单中选择 Copy 命令，然后再右击并在快捷菜单中选择 Paste 命令，将复制的 Pair 粘贴多份，如图 7-13 所示。

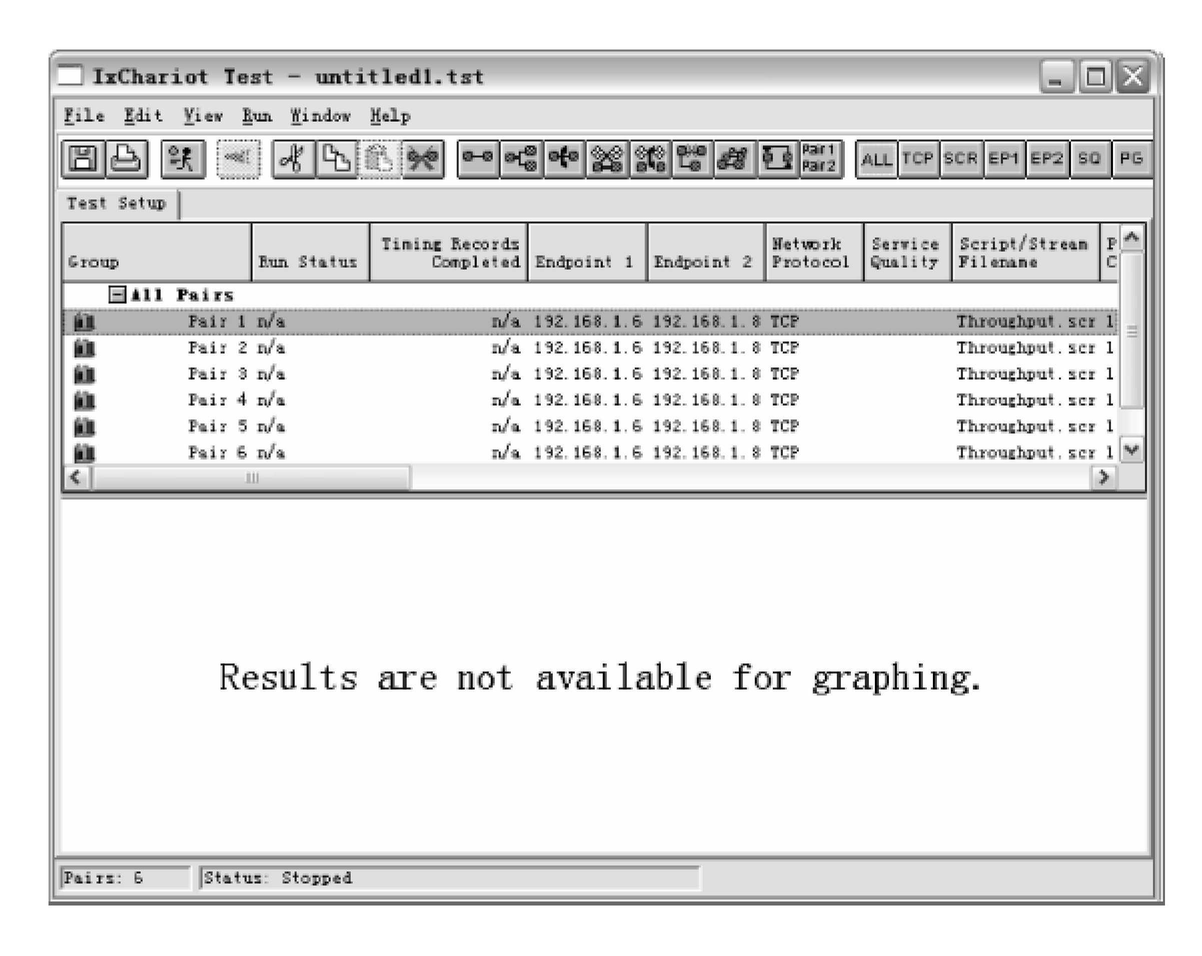


图 7-13　将 Pair 复制多份

③ 单击 Run 按钮，即可开始测试，IxChariot 会测试每对的带宽值，将这些测量结果相加所得到的值，就是带宽的真实值，并显示在 All Pairs 行中，如图 7-14 所示。在曲线图形表中分别用不同颜色的曲线表示每对 Pair 的测试情况。

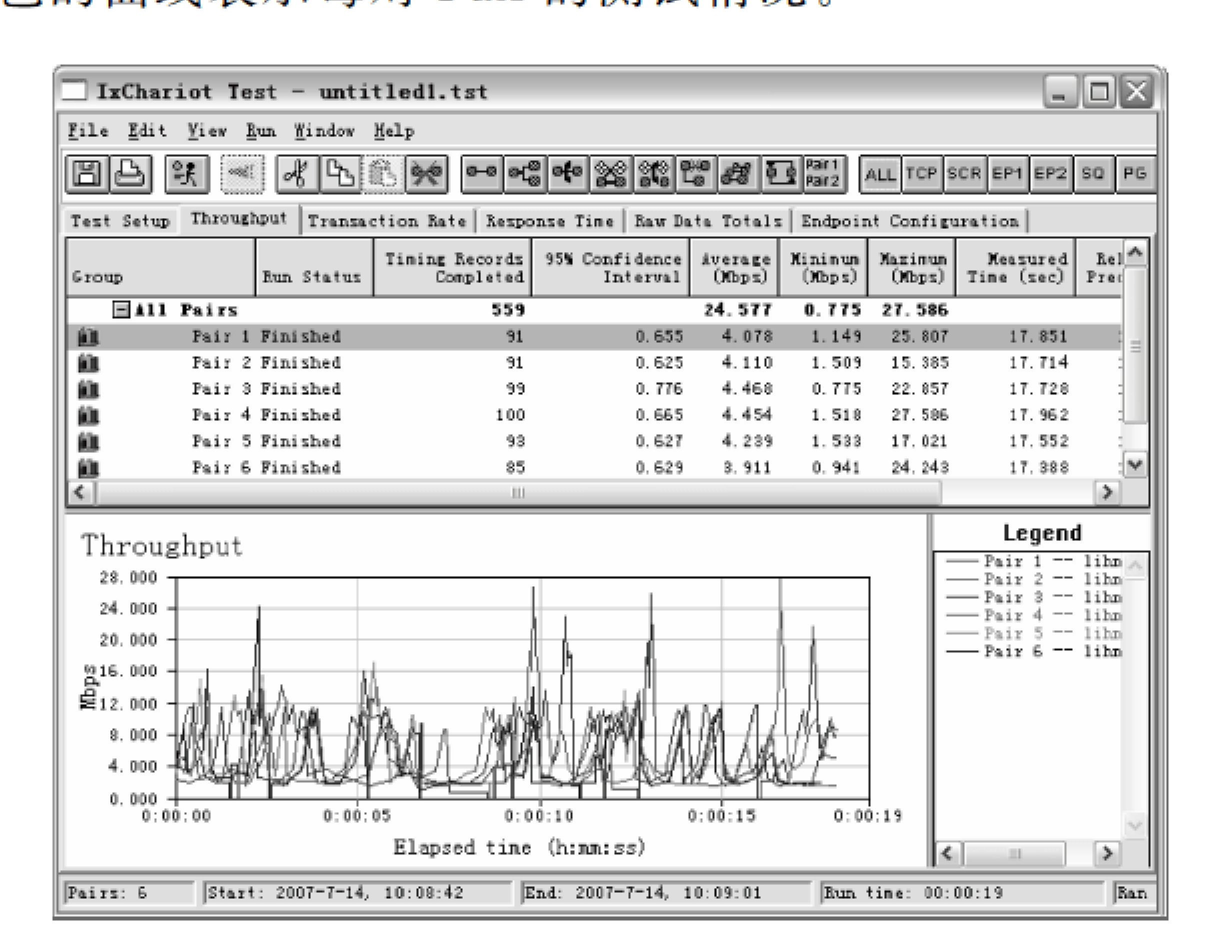


图 7-14　测试结果

（2）大数据包测量法

默认情况下，测量数据包大小只有 100KB，当在网络带宽比较大的网络中进行测量时，其所得到的测量结果是不太准确的。为了提高测量的精确度，需要修改默认数据包的大小，使测量结果更准确。

① 在 IxChariot Test 窗口中，单击 Add an Endpoint Pair 按钮，创建一个 Pair。单击 Select Script 按钮，选择 Throughput 脚本。然后，单击 Edit This Script 按钮，显示图 7-15 所示的 Script Editor - Throughput. scr 窗口。

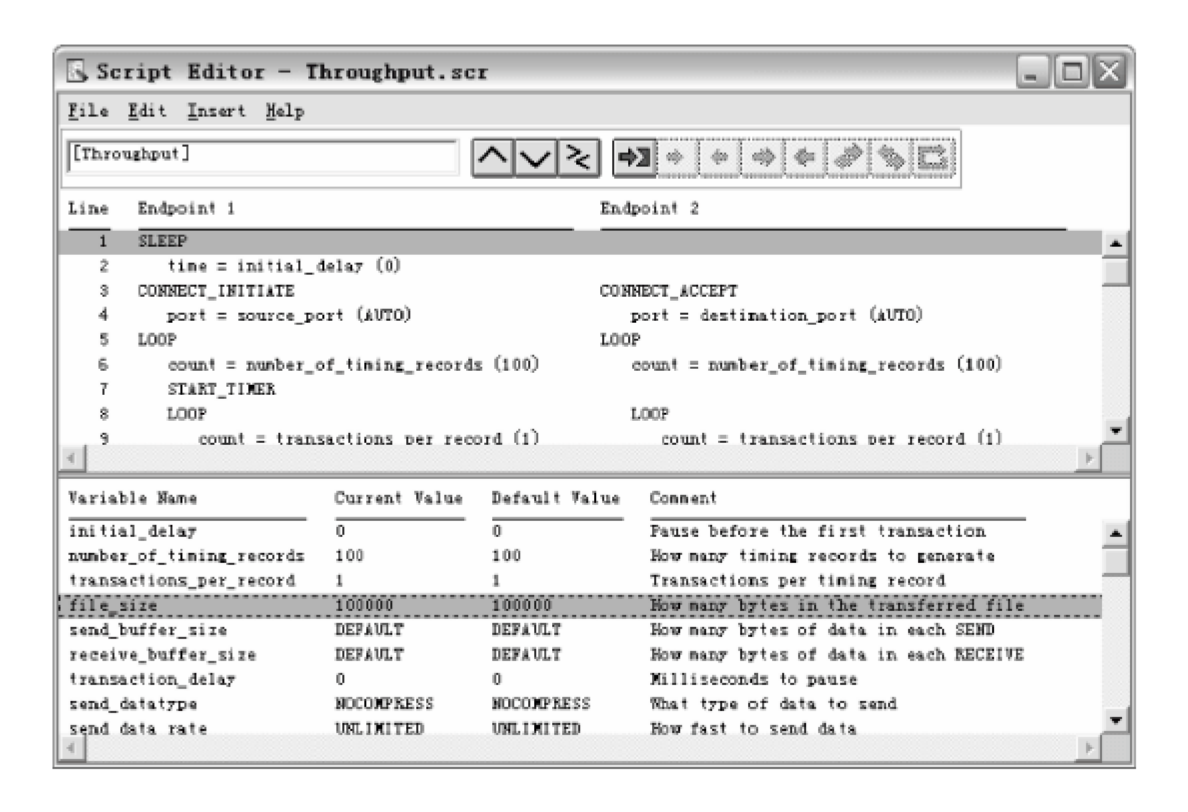


图 7-15　Script Editor - Throughput. scr 窗口

② 在下方窗格中右击 file_size 字段，在快捷菜单中选择 Edit 命令，显示图 7-16 所示的 Edit Variable - file_size 对话框，在 Current value 文本框中显示的就是该脚本文件的大小，以字节(byte)为单位，默认为 100000，即 100KB。修改该数值即可，例如改成 10000000，即 10MB。

③ 单击 OK 按钮，保存修改并关闭 Script Editor - Throughput. scr 对话框，显示图 7-17 所示的提示框，提示是否保存对 Throughput. scr 文件的修改。

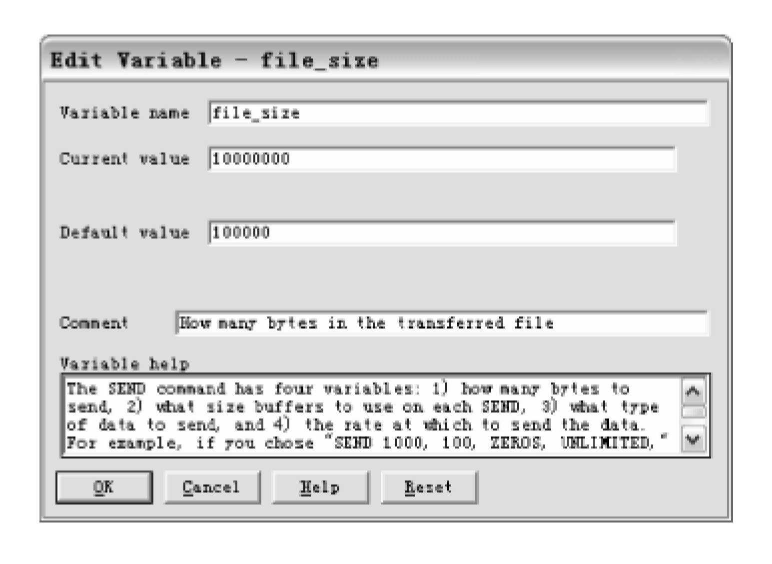


图 7-16　改变数据包的大小



图 7-17　提示框

④ 单击 Yes 按钮保存，返回 Add an Endpiont Pair 对话框，单击 OK 按钮。

⑤ 单击 Run 按钮，即可使用设置好大小的数据包进行带宽测试。当然，数据包越大，测试所需的时间也就越长。

7.3　网络流量监控与分析

无论网络性能有多好，都有可能因为某些用户滥用网络资源，导致网络性能下降，甚至网络瘫痪。因此，管理员应时刻关注网络中的流量情况，保证用户可以充分、合理地利用网络资源，杜绝用户对网络资源的恶意占用。

7.3.1　流量统计分析利器——CommView

CommView 是一款功能强大的工具，可以用来捕获 Internet 和局域网中传输的数据，收集网络传输中的每个信息包，也可以显示信息包和网络连接列表、关键统计信息、协议分布图等重要信息，并可显示内部及外部 IP 地址、端口、主机名称、各种数据的数量等重要资料。管理员可以分析各种 IP 协议，分析网络性能。CommView 的过滤器功能还可以只过滤需要的数据包。CommView 可以运行于 Windows 9x/NT/2000/XP/Vista 等操作系统，用户可以从其官方网站（http://www.tamos.com/）上下载。

1. CommView 的安装与运行

通常情况下，为了使 CommView 能够捕获到网络中的数据，建议将其安装在网络的网关计算机上，如安装代理服务器。如果网络使用路由器，则应使用端口映射，将路由器端口映射到 CommView 计算机上即可。CommView 的安装操作比较简单，大部分操作只需单击 Next 按钮即可，这里就不再赘述。

（1）双击桌面上的 CommView 图标运行软件，显示图 7-18 所示的对话框。提示需要安装 CommView 驱动程序。

CommView

CommView will now install the drivers. This will take between 10 and 60 seconds. Windows may ask you for confirmation one or several times.

确定

图 7-18　提示安装 CommView 驱动程序

（2）单击“确定”按钮，即可完成安装。安装完成后，显示图 7-19 所示的对话框，询问是否安装 RAS 拨号适配器，单击“是”按钮安装，单击“否”按钮则不安装。

（3）单击“否”按钮，显示图 7-20 所示的提示框，显示欢迎信息。

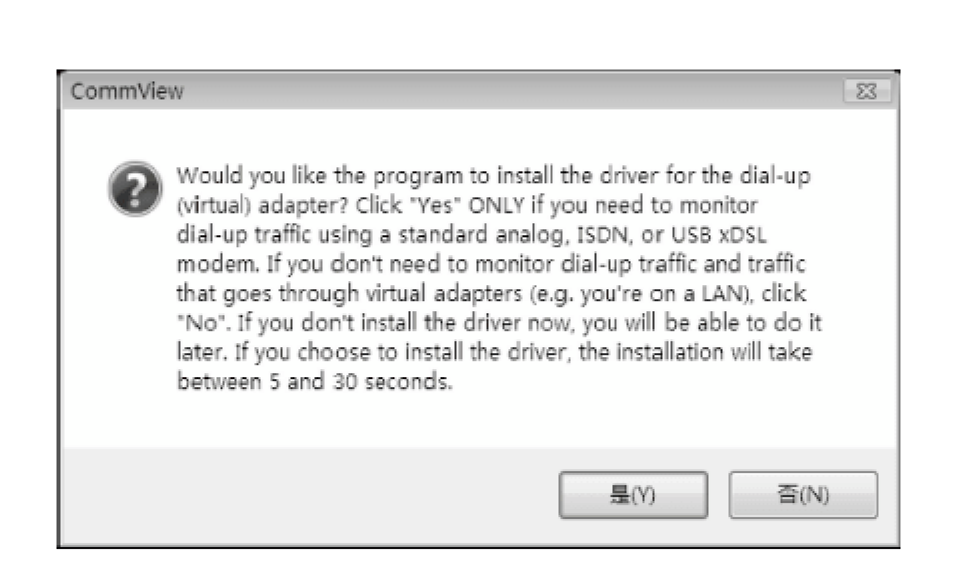




图 7-19　提示安装 RAS 拨号适配器

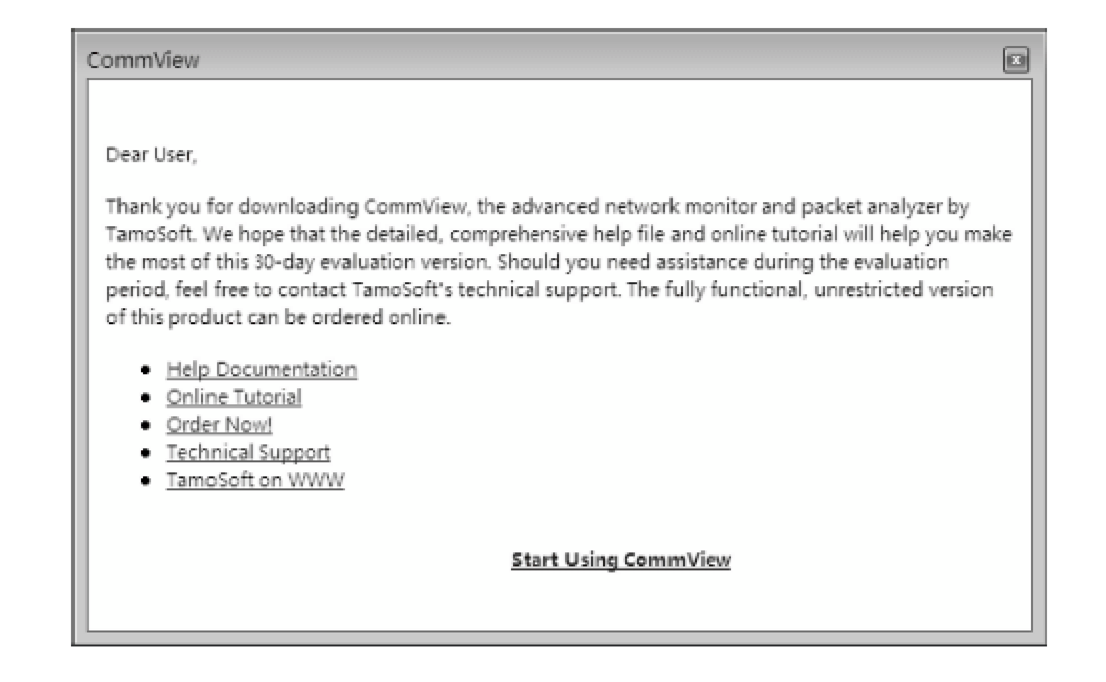


图 7-20　欢迎界面

（4）单击 Start Using CommView 链接，显示 CommView 主窗口，如图 7-21 所示。

如果当前计算机安装了多个网卡，各个网卡连接不同的网段，则应先从工具栏上的下拉列表框中选择与要监控的网络相连的网卡，这样才能正确地捕获网络中的数据。

2. 捕获并分析网络数据

CommView 可以捕获局域网中所有计算机与外部网络间传输的数据，通过分析这些数据，管理员可以清楚地了解到网络的运行状况，如果网络出现了故障，还可以迅速找出故障所在。

（1）在 CommView 窗口中，单击工具栏上的 Start Capture 按钮，或选择 File 菜单中的

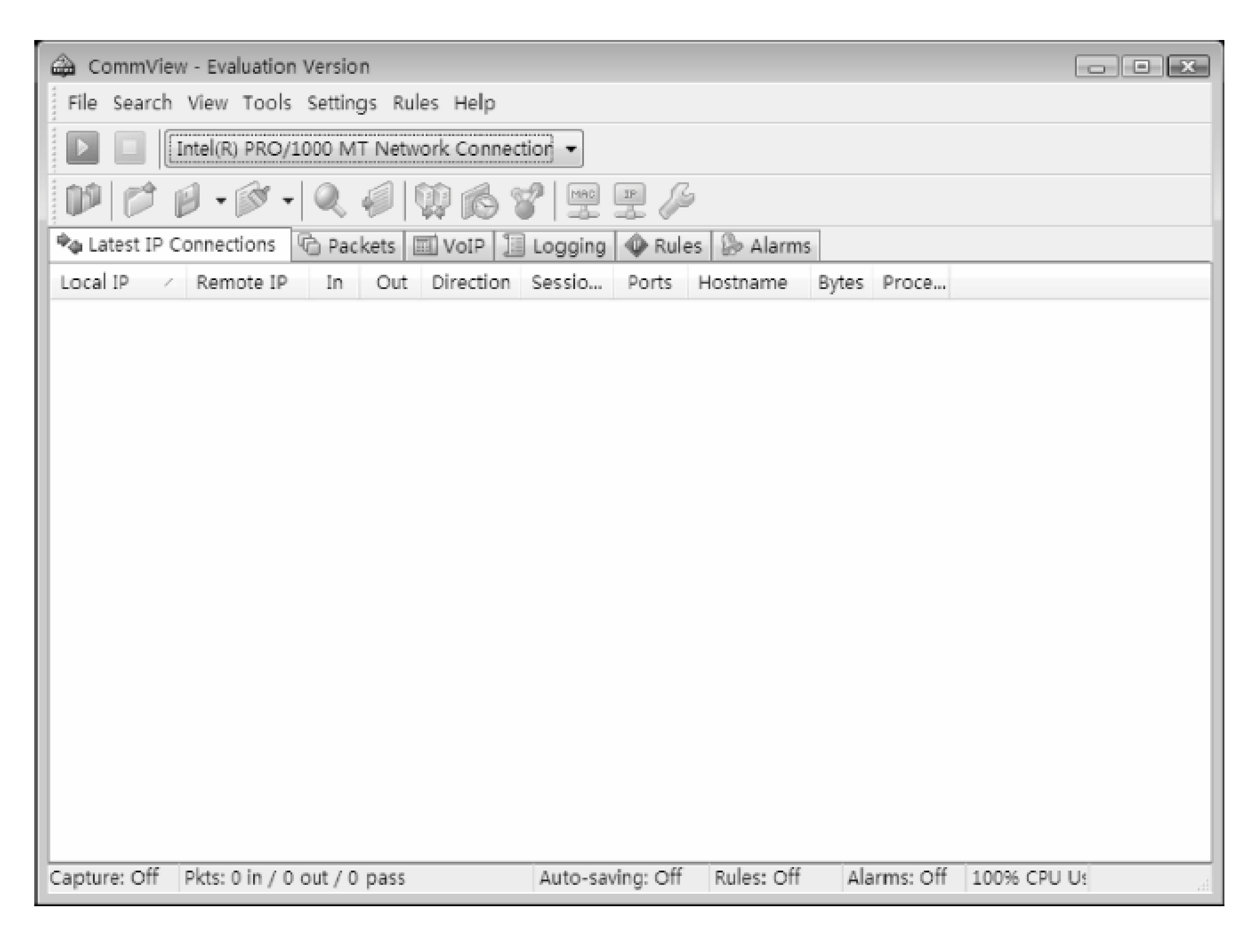


图 7-21 CommView 窗口

Start Capture 命令，CommView 便开始捕获网络内传输的数据，如图 7-22 所示。ComView 捕获的数据信息非常详细，Latest IP Connections 选项卡中显示了各个网络连接的各种信息，包括本地 IP 地址（Local IP）、远程 IP 地址（Remote IP）、传入的数据量（In）、传出的数据量（Out）、数据传输方向（Direction）、会话时间（Sessions）、端口（Ports）、主机名（Hostname）、传输字节数（Bytes）、使用的进程名称（Process）。另外，还会以国旗的方式显示远程 IP 地址所在的国籍。

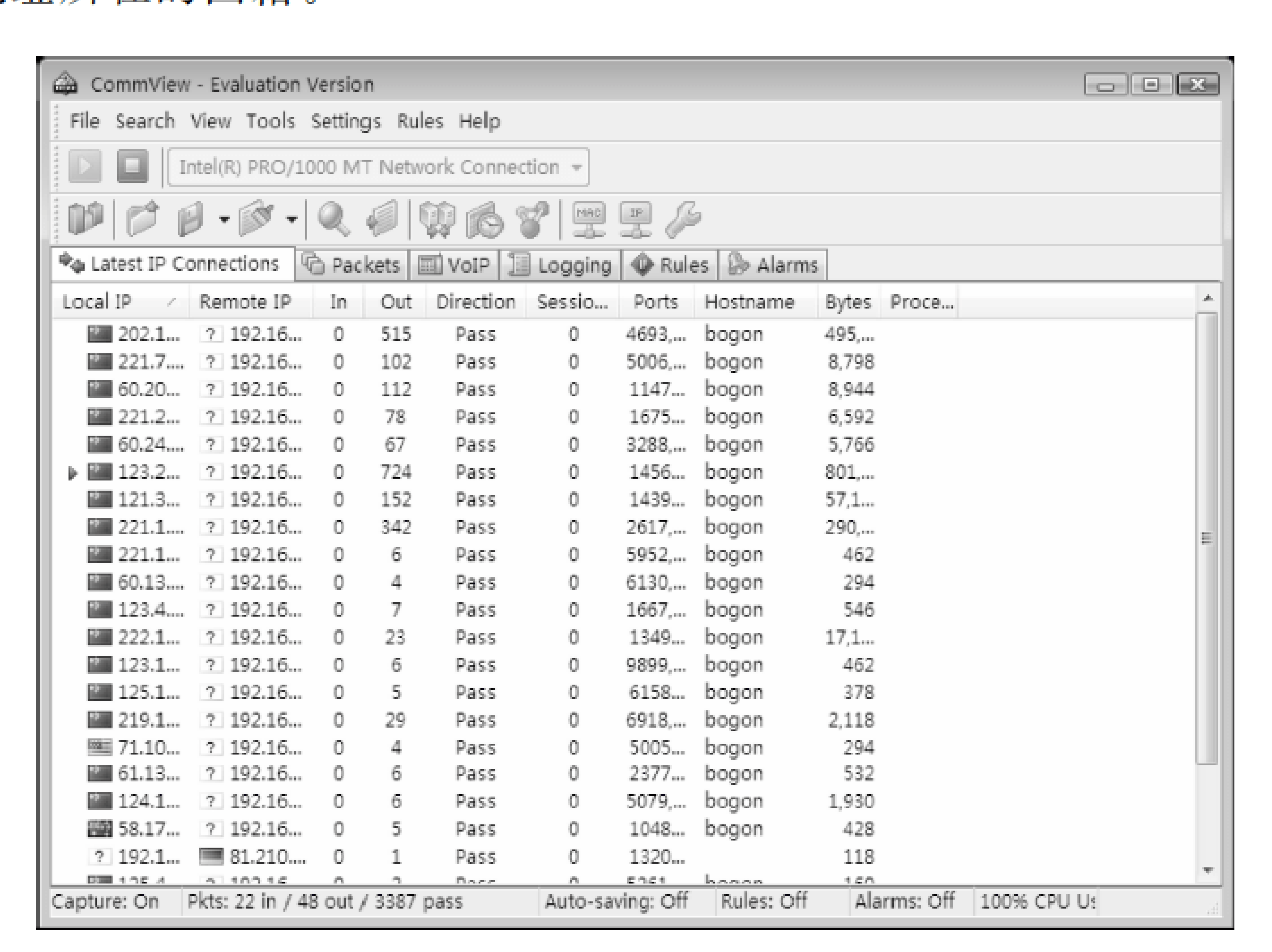


图 7-22 捕获数据

（2）当捕获到一定的数据后，单击工具栏上的 Stop Capture 按钮即可停止捕获，此时即可对所捕获到的数据进行分析。通过这些信息，管理员可以清楚地看到网络中哪台计算机正在与外部网络的哪些地址进行通信，有哪些可疑端口正在使用等，从而迅速地找到问

题所在，例如，通过查看端口即可得知，使用 8000、4000 端口的用户正在使用 QQ，端口为 mirosoft-ds 则表示用户正在访问共享文件。

(3) 选择 Packets 选项卡，在这里可以看到每个数据包的详细信息。此处共分为 3 个窗格，最上面的窗格中显示了传输数据的源地址和目的地址的网卡 MAC 地址、端口以及时间。中间的窗格为“Hex 窗格”，这里是以十六进制代码显示的信息，如图 7-23 所示。在 MAC Addresses 列表中，不仅显示网卡的 MAC 地址，也显示了网卡的型号或名称。

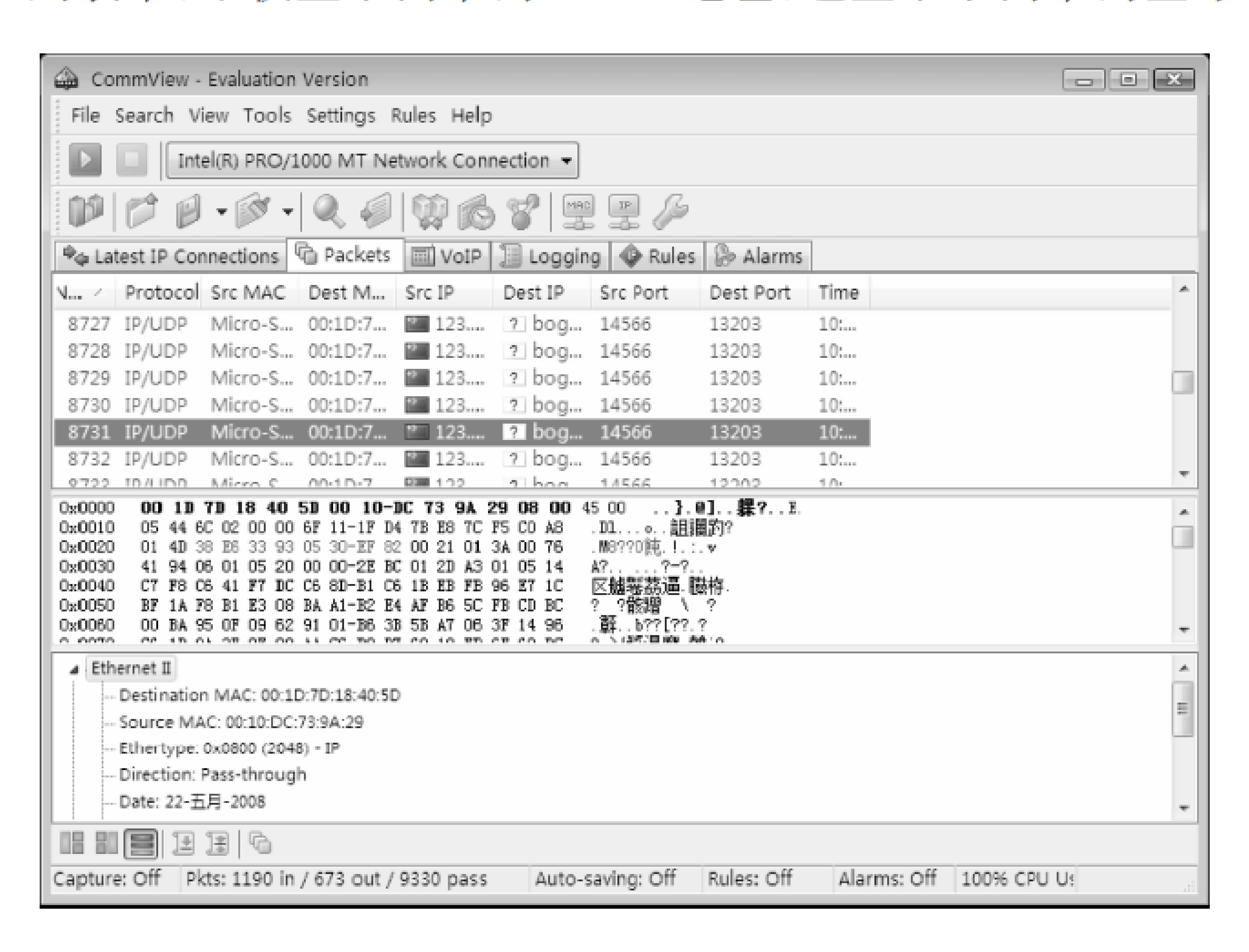


图 7-23　Packets 选项卡

最下面的窗格中显示了所使用的传输协议的详细信息，也是网络管理员最需要注意的地方。在 Ethernet 选项区域中，显示信息(如图 7-24 所示)主要包括如下内容。

(1) Destination MAC：目的地址网卡的物理地址。

(2) Source MAC：源地址网卡的物理地址。

(3) Ethertype：以太网类型。

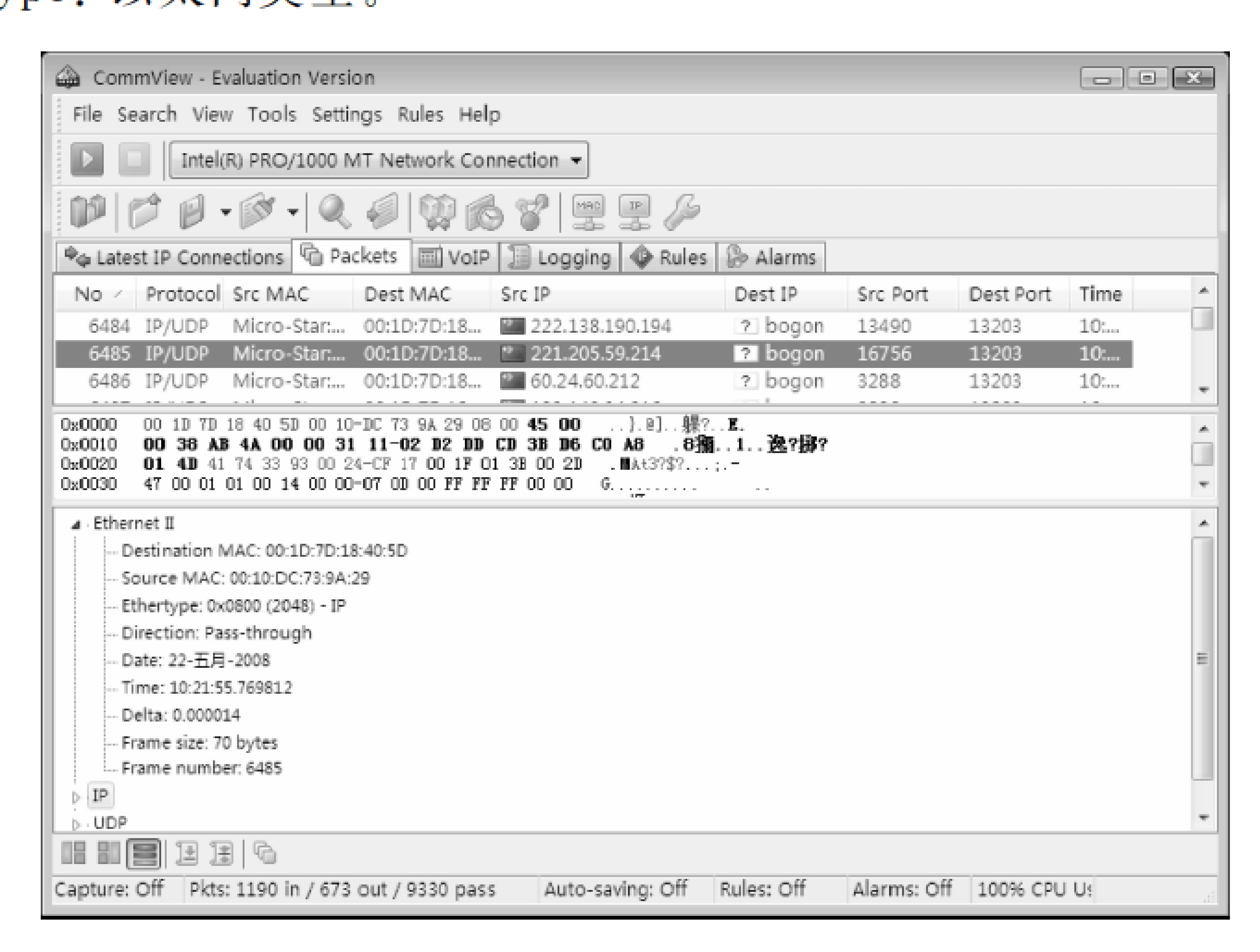


图 7-24　Ethernet 选项区域

（4）Direction：数据包传输方向。

（5）Date：数据传输日期，Time 中显示的则是传输的时间。

（6）Frame size：每个帧的大小。

（7）Frame number：帧的总数量。

在 Ethernet 选项区域下面是 IP 列表，显示的 IP 文件头信息（如图 7-25 所示）主要包括如下内容。

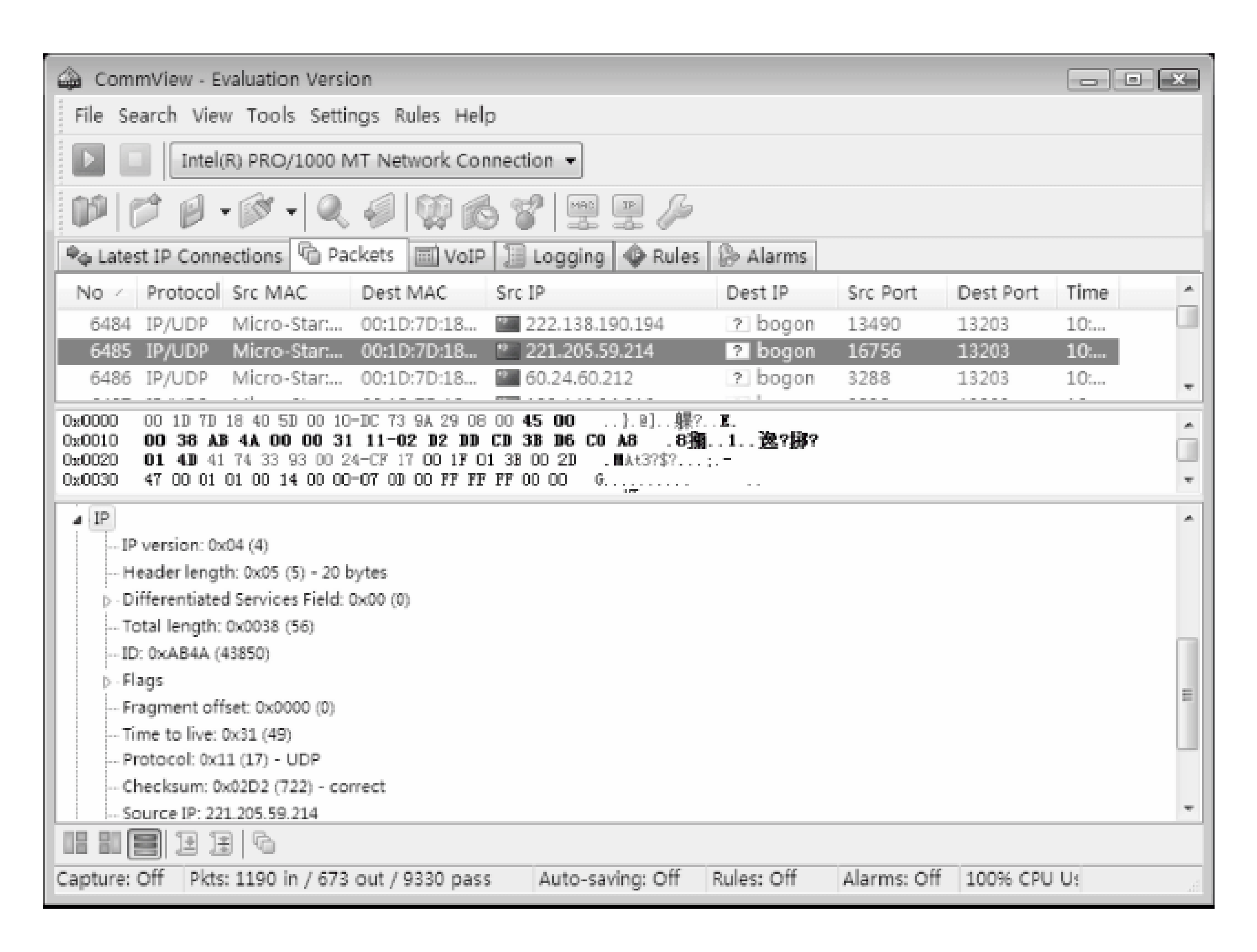


图 7-25　IP 文件头信息

（1）IP version：以十六进制显示所使用的 IP 版本号，这里为 4，即所使用的 IP 版本号为 IPv4，如果为 6 则表示是 IPv6。

（2）Header length：Internet 文件头的长度，为 20 个字节。

（3）Flags：数据报的“标记”功能，例如，数据报分段用 0 标记，未分段用 1 标记。

（4）Fragment offset（分段差距）：用来说明某个区段属于数据包的哪个部分。分段差距为 0 个字节。可以设定 0 代表最后一段，或者设定 1 代表更多区段。此处值为 0。

（5）Time to live：数据包的生存时间，表示 TTL 值的大小，说明一个数据包可以保存多久。

（6）Protocol：数据所使用的协议。

（7）Checksum（校验和）：校验和（只在这个文件头中使用）的值，并且已经做了标记，表明这个数值是正确的。

（8）Destination IP：数据访问的目的地址。

（9）Source address：数据的来源地址。

在 IP 文件头信息下面为协议信息，根据所捕获的数据不同，显示 TCP、UDP 或 ICMP 文件头信息等。在 TCP 协议中的显示信息（如图 7-26 所示）主要包括如下内容。

（1）Source port：使用 TCP 协议的网络连接的源端口。

（2）Destination port：使用 TCP 协议的网络连接的目的端口。

（3）Sequence：该帧的排列顺序。

（4）Acknowledgement：该帧的应答信息。

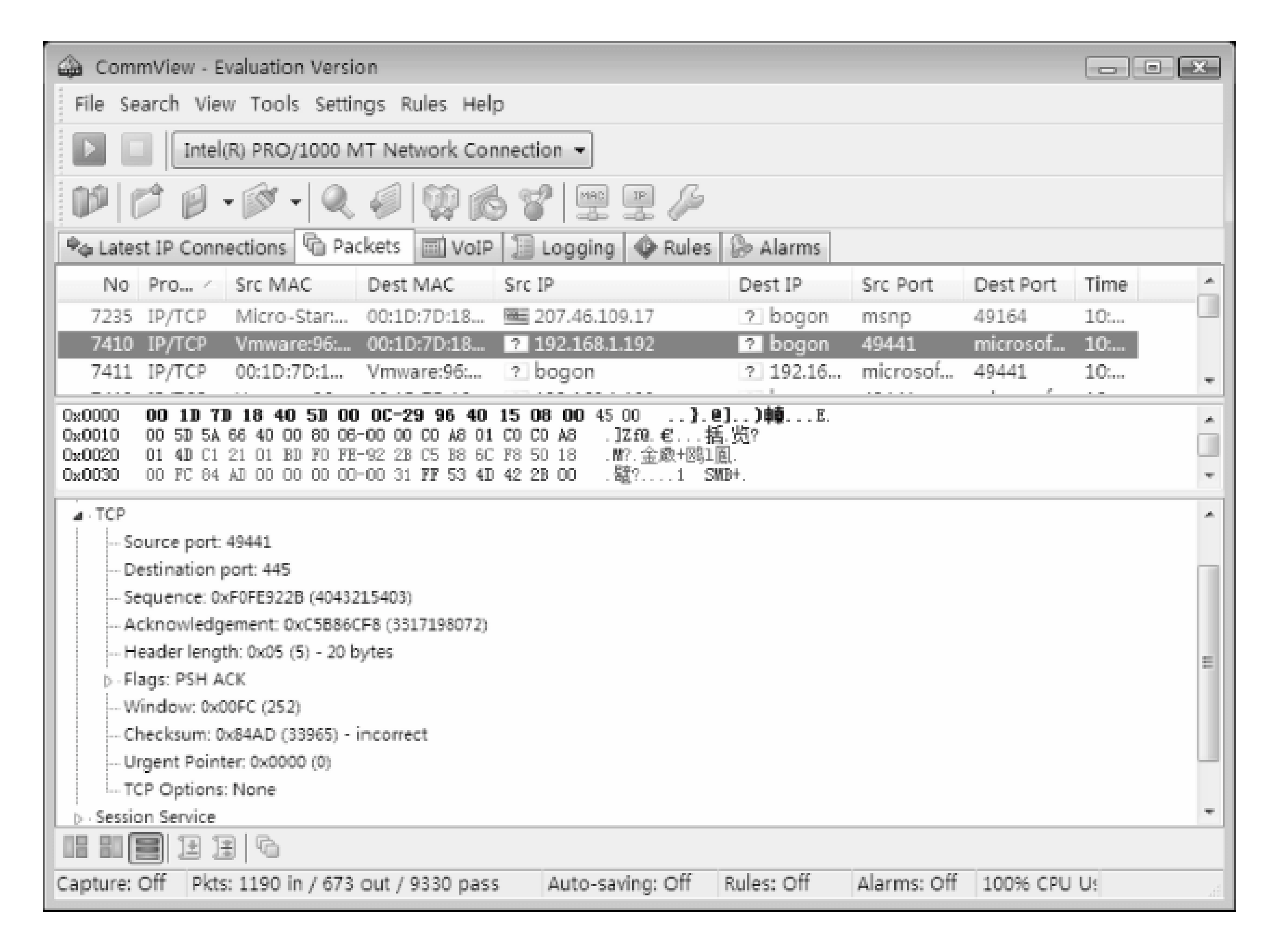


图 7-26　TCP 文件头信息

（5）Header length：该 TCP 协议的头长度。

（6）Checksum：TCP 文件头校验和的值。

如果所使用的协议为 UDP，则在下方会显示 UDP 文件头信息，如图 7-27 所示。

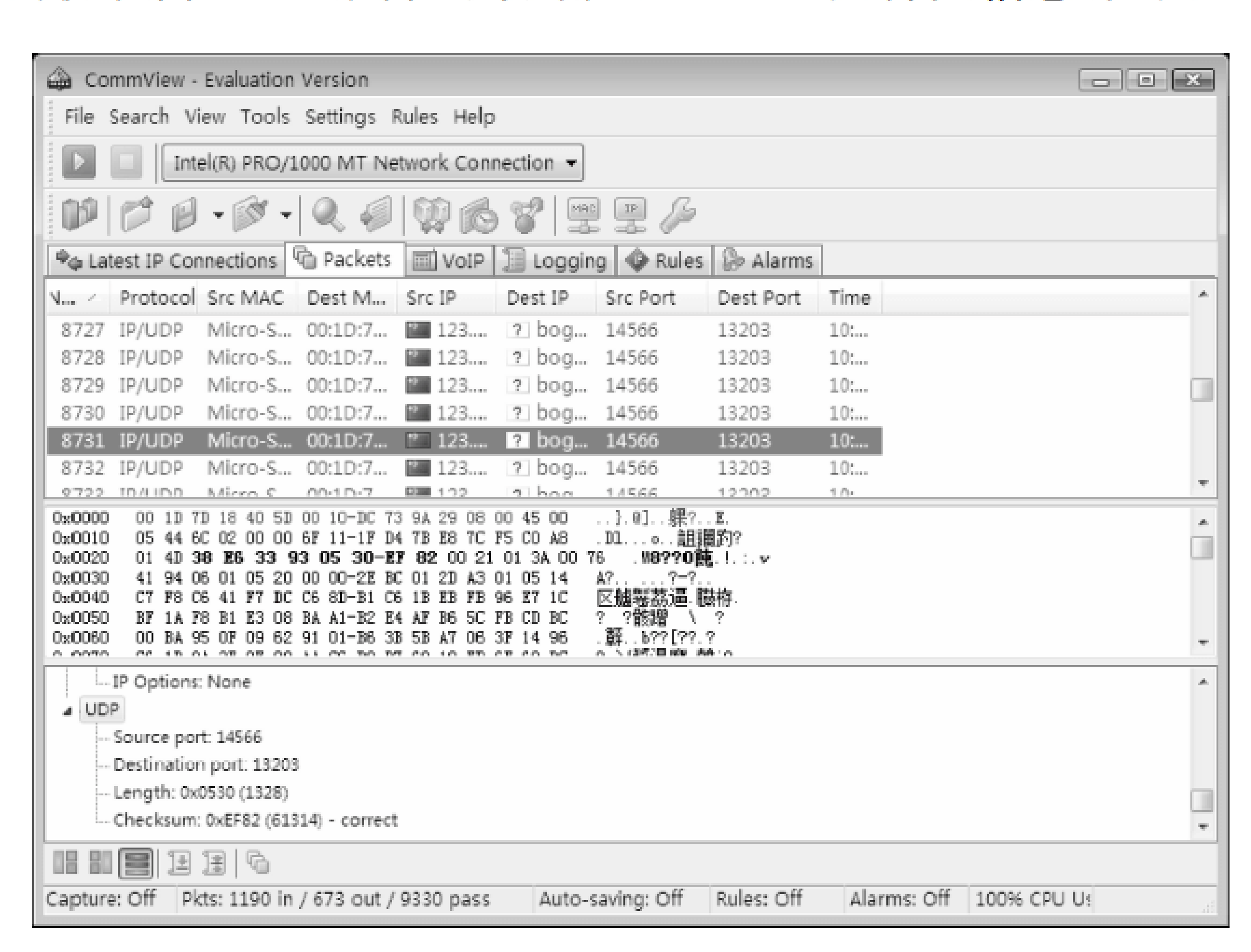


图 7-27　UDP 文件头信息

（1）Source port：使用 UDP 协议的网络连接的源端口。

（2）Destination port：使用 UDP 协议的网络连接的目的端口。

（3）Length：UDP 文件头的长度。

（4）Checksum：UDP 协议校验和的值。

通过对协议信息进行分析，网络管理员可以了解网络状况及数据来源。

3. 查看网络传输状态

在捕获数据的过程中，不仅可以查看网络中各台计算机所传输的数据包，还能以图形方式查看网络中各种协议的使用状况及数据传输状态，并根据这些数据分析网络中是否有蠕

虫、木马或网络风暴占用带宽，从而迅速找出网络故障发生的原因。

当捕获数据完成以后，依次选择 View→Statistics 命令，或者单击工具栏上的 Statistics 按钮，显示图 7-28 所示的 Statistics 窗口。默认在左侧列表中选中 General 选项，在这里以图形形式显示了网络的使用状况，如数据包的传输速率(Packets per second)、当前传输的字节数(Bytes per sec.)、网络利用率(Current network utilzation)等，并在最下方的 Total 中显示了传输的数据包总数(packets)和字节总数(bytes)，这些信息的显示比单纯的数值方式更清楚。

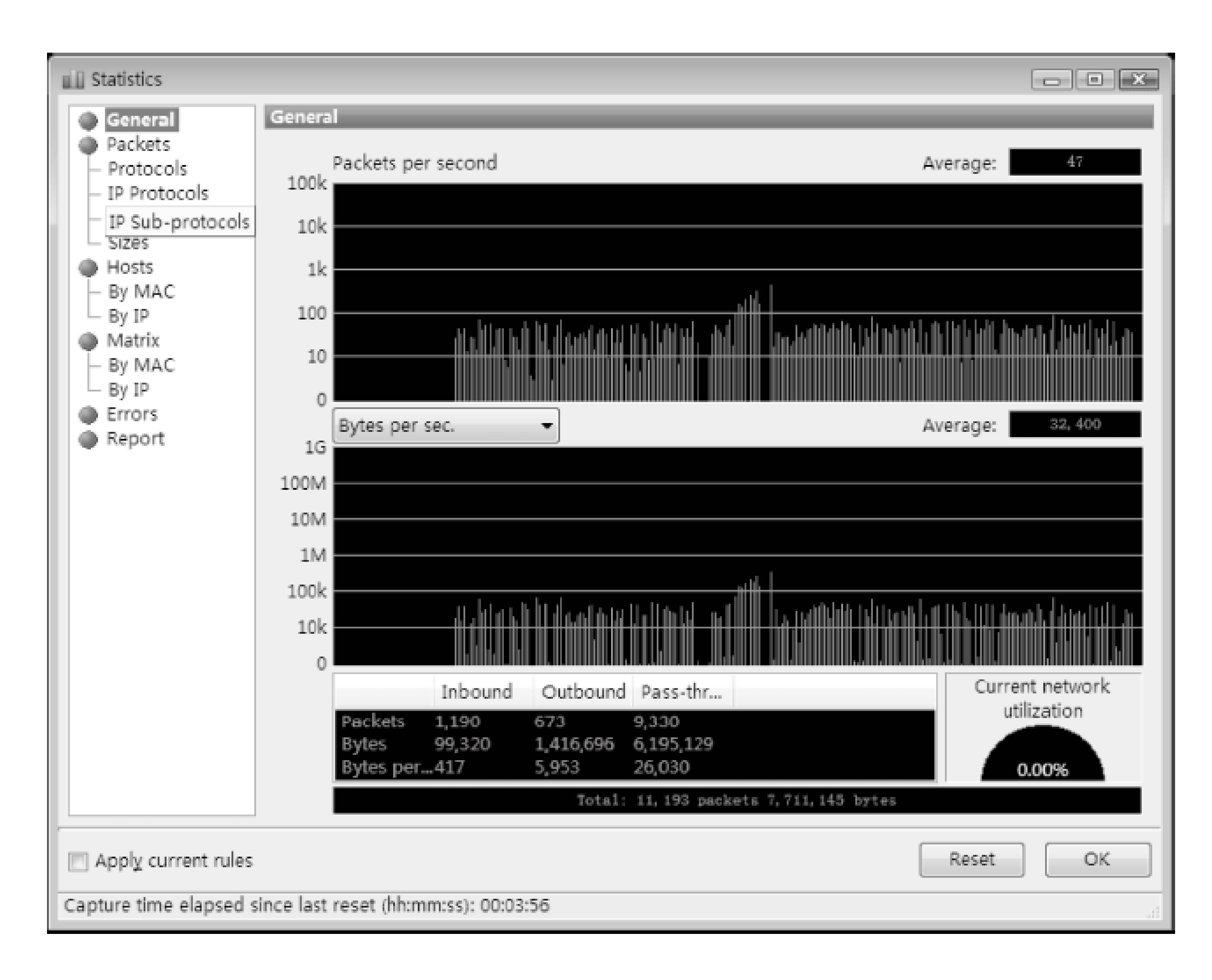


图 7-28 查看网络传输状态

在左侧列表中选择 Packets 选项，即可查看各种数据包协议的传输状态。在 Packets Protocols 窗口中，以圆饼图显示了各种协议的使用状态，如图 7-29 所示。使用不同的颜色

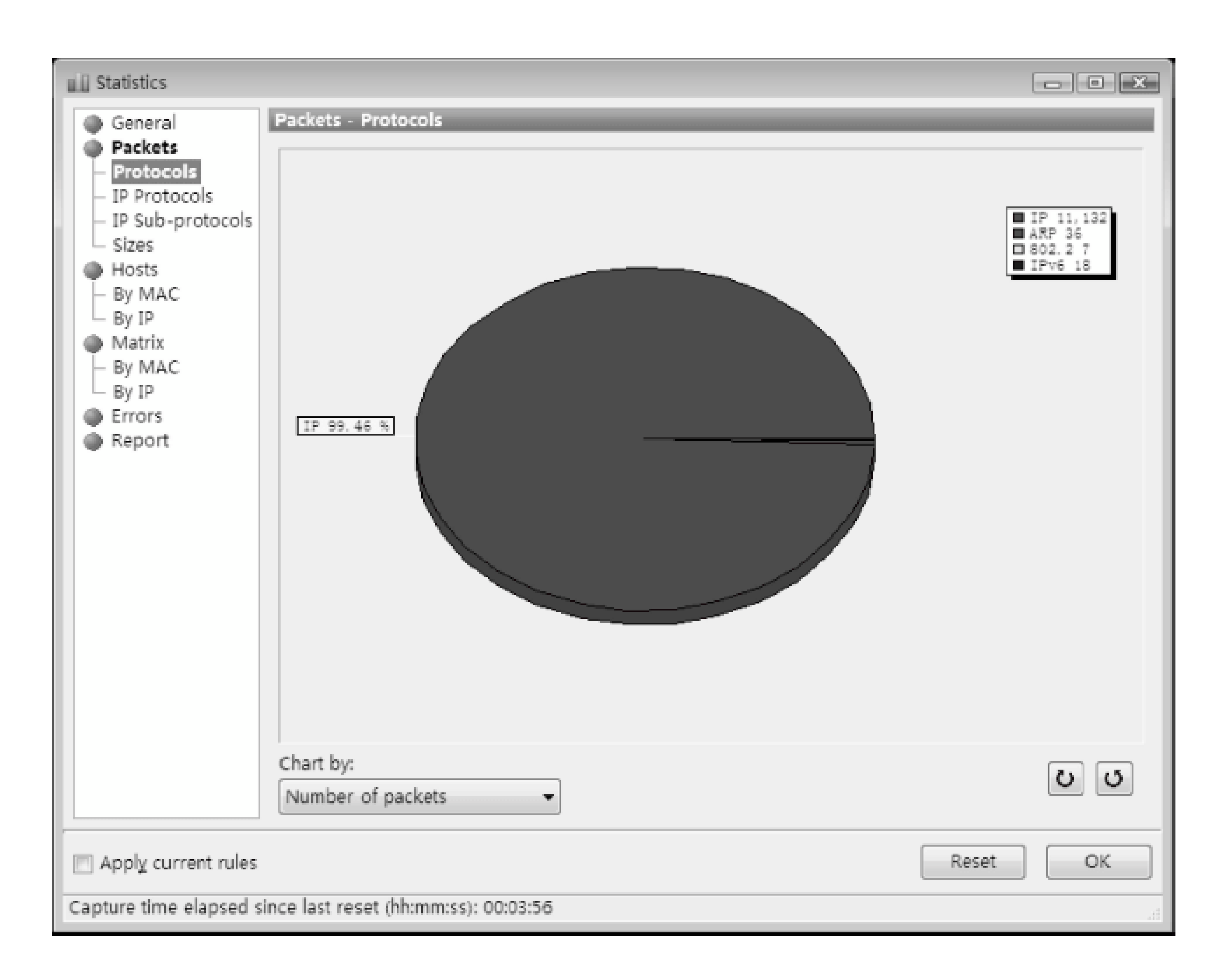


图 7-29 协议使用情况

代表不同的协议，如 IP、ARP、NetBIOS、IPX 等协议。根据这些协议的使用率，就可以了解网络传输状态，例如，网络中网速特别慢，而在该窗口中发现 ARP 使用率特别高，这就有可能是网络风暴所致，必须及时解决故障。

在 Protocols 列表中选择 IP Protocols 选项，显示了 TCP、UDP、ICMP 和 IGMP 等协议的利用率，如图 7-30 所示。

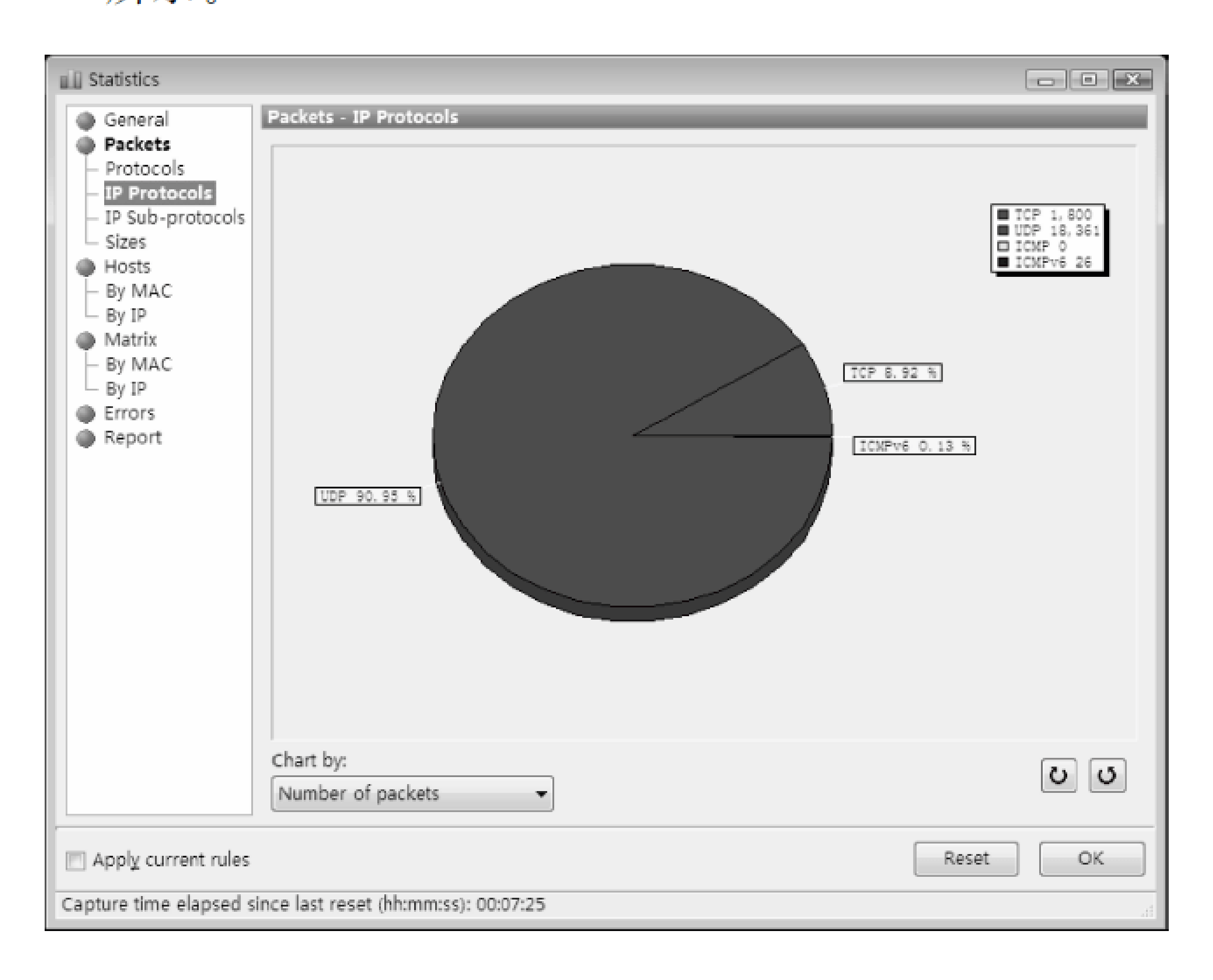


图 7-30　IP Protocols 选项

在 Protocols 列表中选择 IP Sub-protocols 选项，显示了各种网络服务的使用情况，如 HTTP、FTP、POP3、SMTP、Telnet、NNTP、NetBIOS、HTTPS 和 DNS 服务等，如图 7-31 所示。

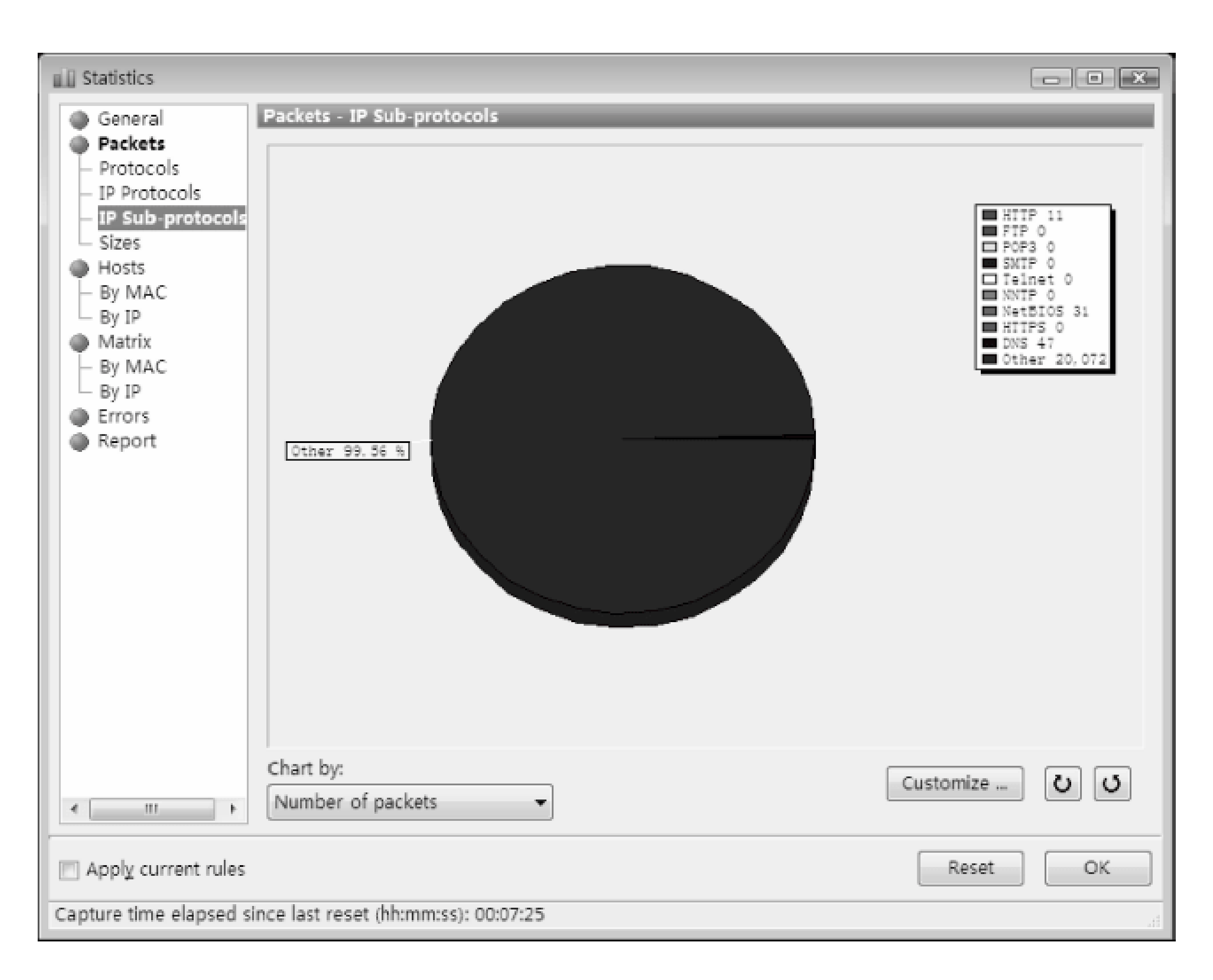


图 7-31　IP Sub-protocols 选项

在 Protocols 列表中选择 Sizes 选项，显示了各种不同字节的数据包的传输情况，包括小于 64B、66～127B、128～255B、256～511B、56～1023B 以及大于 1024B 的数据包，如图 7-32 所示。

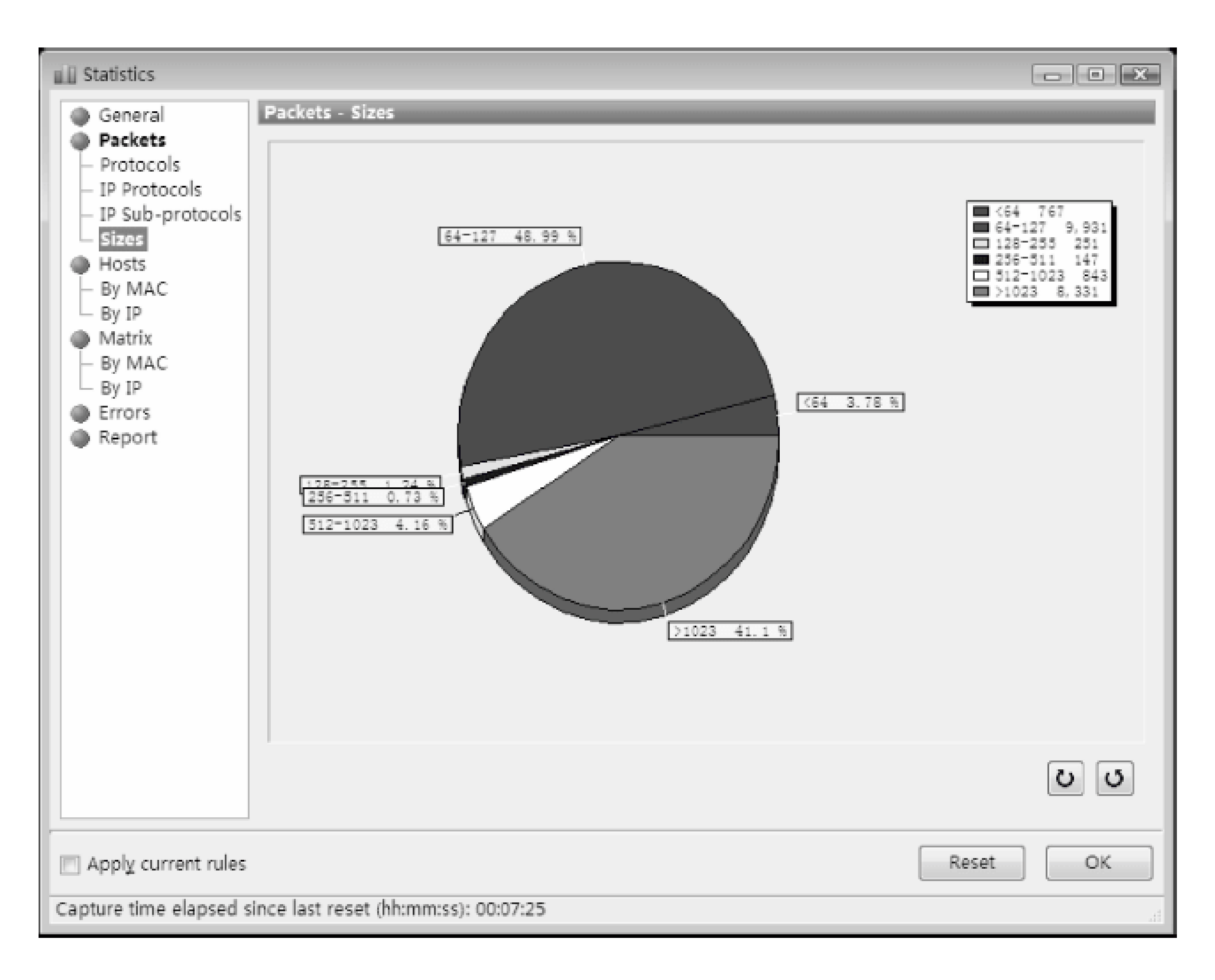


图 7-32　Sizes 选项

在左侧列表中选择 Hosts By MAC 选项，显示了各个网卡的 MAC 地址，并列出了各个网卡所发送和接收的数据包、字节数量，如图 7-33 所示。

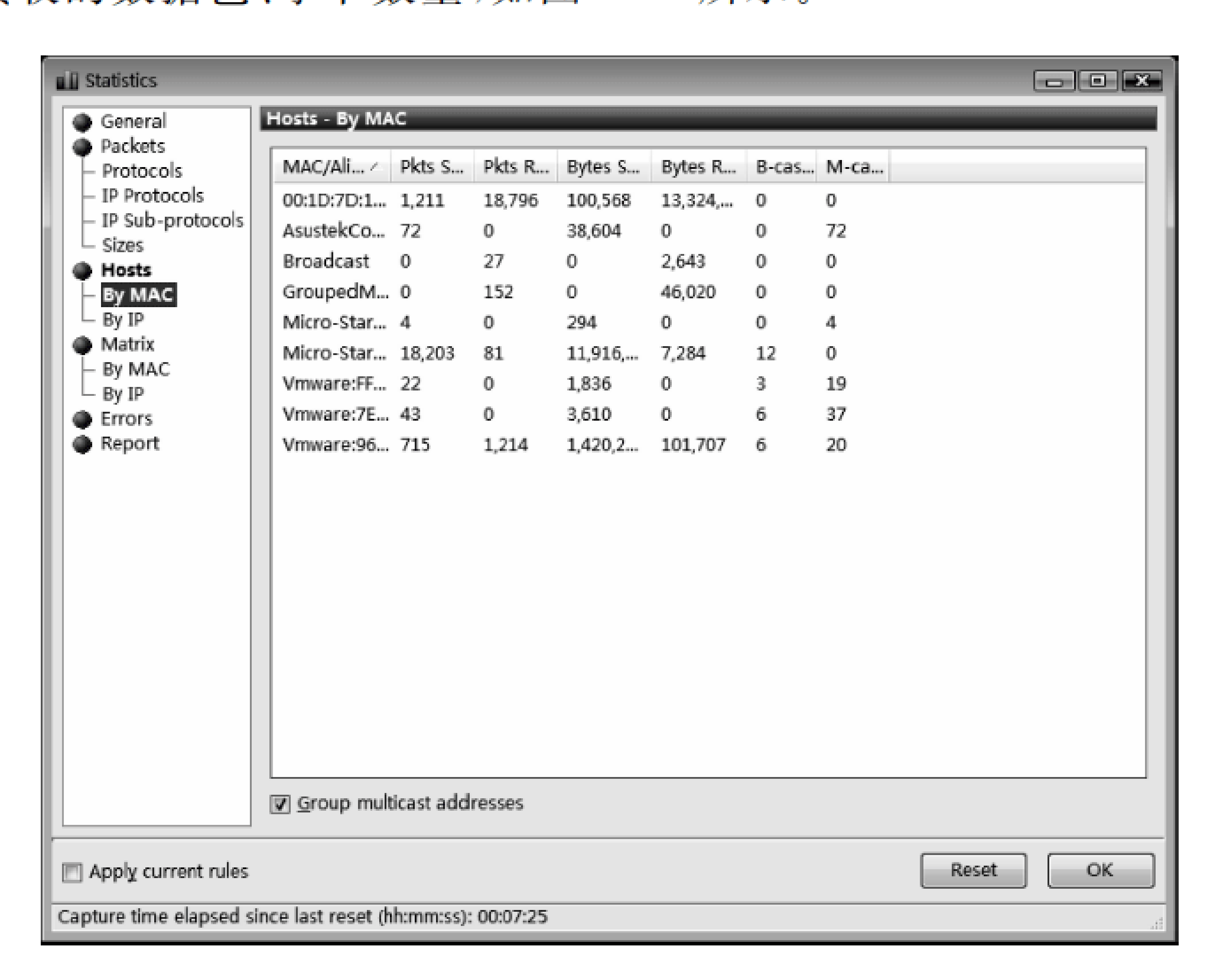


图 7-33　Hosts By MAC 选项

在左侧列表中选择 Matrix 选项，然后选择 By IP 选项，将以矩阵方式列出当前网络中有哪些 IP 地址正在连接，如图 7-34 所示，并且使用连线将正在连接的计算机连接起来，便于管理员查看。默认情况下，矩阵中只显示 10 个活动最多的节点，如果想多显示一些，可以在 Most active pairs 文本框中输入欲设置的值。默认没有显示广播和多播的连接，如果想

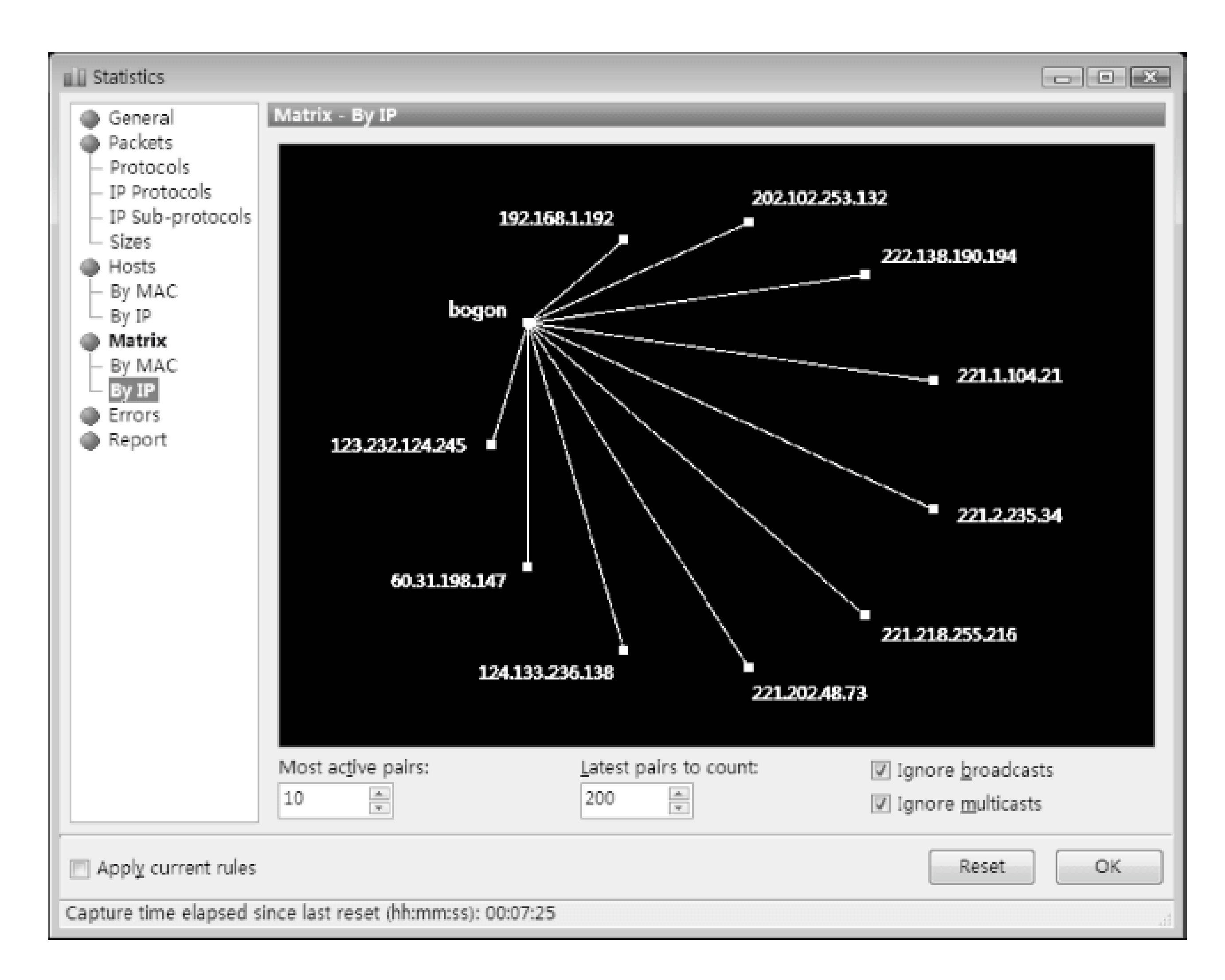


图 7-34　查看 IP 地址连接情况

显示这些内容，取消选中 Ignore broadcasts 和 Ignore multicasts 复选框即可。

在 Errors 窗口中显示了网络中错误的传输数据；Report 窗口中可将当前捕获结果作为报告，输出成 HTML 网页格式进行保存。

通过端口可以更容易了解到某个连接正在干什么，但如果不知道某个端口的作用以及端口会被哪些协议使用，可选择 View 菜单中的 Port Reference（端口参考）命令，显示图 7-35 所示的 Port Reference 窗口。在该窗口中列出了大部分常用端口的信息，例如各个端口所使用服务、协议等，在分析网络数据时可作为参考。

Port Reference

Port	Service	Protocol	Comment
7	echo	tcp	
7	echo	udp	
9	discard	tcp	
9	discard	udp	
11	systat	tcp	Active users
11	systat	udp	Active users
13	daytime	tcp	
13	daytime	udp	
17	qotd	tcp	Quote of the day
17	qotd	udp	Quote of the day
19	chargen	tcp	Character generator
19	chargen	udp	Character generator

图 7-35　Port Reference 窗口

4. 设置过滤器

CommView 虽然可以捕获网络中的所有数据，但有许多数据并不是所需要的，通过设置过滤器，可以根据过滤器中设定的条件，只捕获特定的数据，便于管理员查看分析。

（1）自定义过滤器

通过自定义过滤器，可以捕获网络中管理员所关心的数据，从而解决某些具有针对性的问题，例如广播风暴等。

① 在 CommView 窗口中，选择图 7-36 所示的 Rules 选项卡，在左侧列表中默认选择 Advanced Rules 选项，在右侧栏中选中 Enable advanced rules 复选框，启动过滤器功能。

② 在 Add/Edit Record 选项区域中，选中 Capture packets(inclusive)单选按钮，即只捕获符合该规则的数据包，如图 7-37 所示。如果选中 Ignore packets(exclusive)单选按钮，则不捕获该规则中的数据包。在 Name 文本框中，输入新规则的名称，在 Formula 文本框中，编写该规则的公式，主要是设置要捕获哪些 IP 地址传输的数据，例如，在 Formula 文本框中，输入 sip=192.168.1.77 and dip=192.168.1.10，表示捕获源地址为 192.168.1.77 与

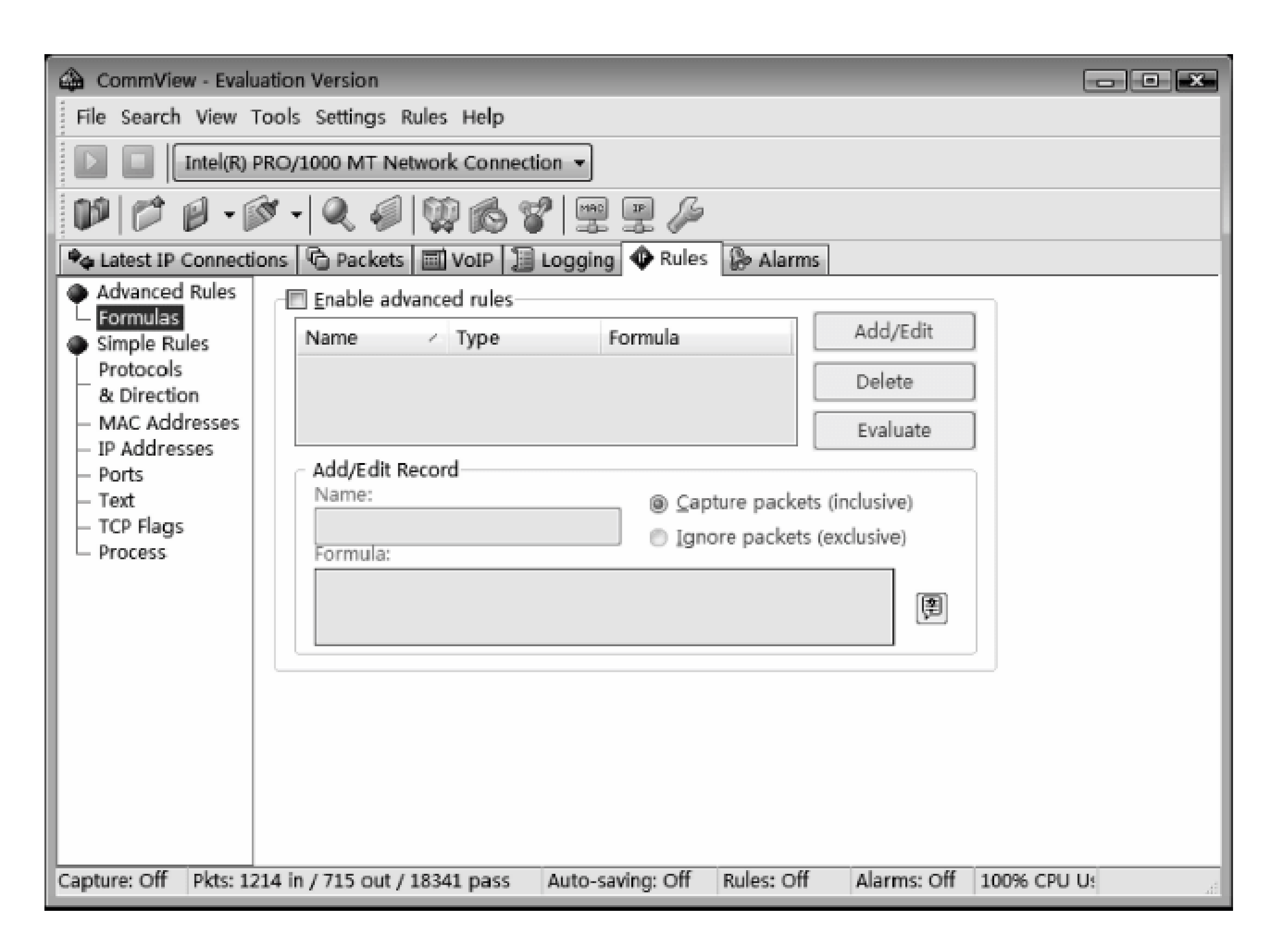


图 7-36　添加过滤器

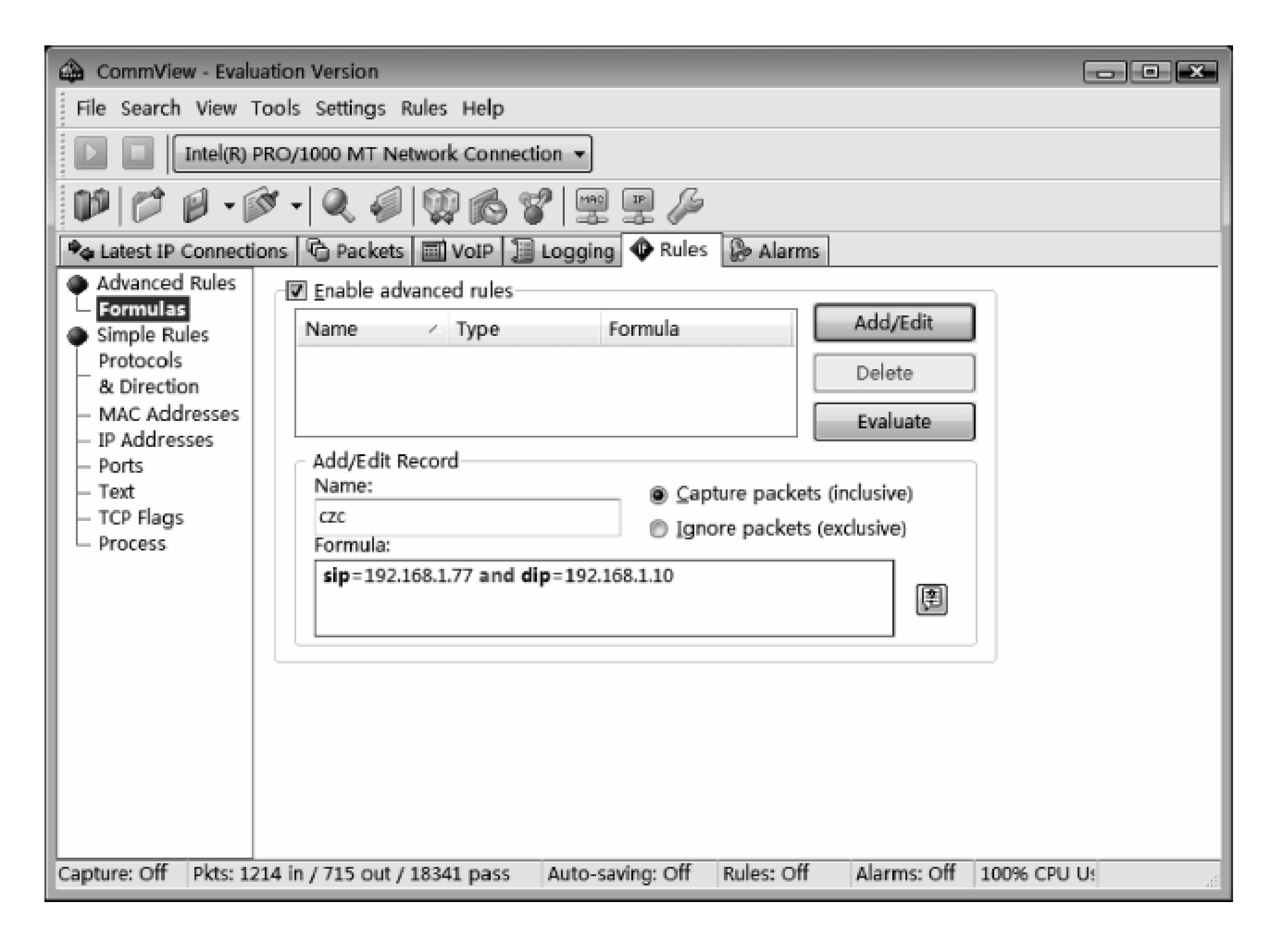


图 7-37　编辑公式

目的地址为 192.168.1.10 传输的数据。其中，sip 表示源地址，dip 表示目的地址，多个条件可使用逻辑关系来连接，如 and、or、not 等。

③ 单击 Add/Edit 按钮，即可将该规则添加到规则列表中，还可以设置详细的条件。

④ 设置完成以后不需保存即可生效，如果想删除某个已添加的规则，右击该规则，在快捷菜单中选择 Clear Select 命令即可。

⑤ 设置完成后单击 Start Capture 按钮，CommView 即可根据此过滤器的设置捕获网络中符合条件的数据了。

（2）简单过滤器

简单过滤器主要是指软件自带的具有某些单一功能的过滤器，通过结合使用多种过滤器，达到分析网络流量的目的。

① Protocols & Direction。在左侧列表中，选择 Protocols & Direction 选项，如图 7-38

所示。在右侧栏中，选中 Enable ethernet protocol rules 复选框，启用以太网协议规则，在 Action 选项区域中选中 Capture 单选按钮，然后在 Description 列表框中选择要捕获的协议。选中 Enable IP protocol rules 复选框，启用 IP 协议规则。其中，Capture inbound packets 复选框表示捕获传入的数据包，Capture outbound packets 复选框表示捕获传出的数据包，Capture pass-through packets 复选框表示捕获传递会话数据包。

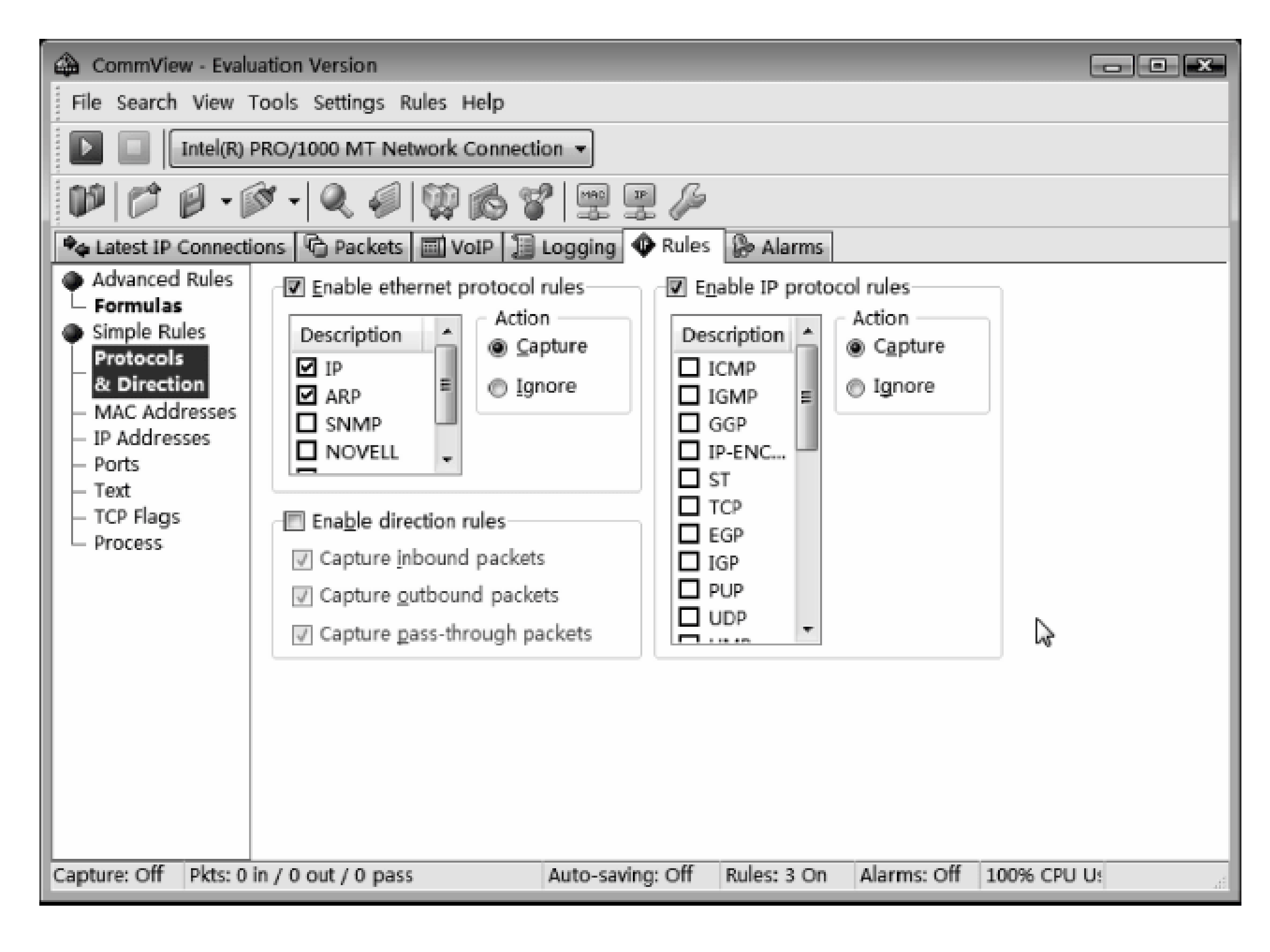


图 7-38　Protocols & Direction

注意：在每种规则中，都会有 Capture 和 Ignore 单选按钮，选择 Capture 就只会捕获符合当前规则条件的数据，而选择 Ignore 单选按钮则对符合当前条件的数据全部放行。

② MAC Addresses。在左侧列表中选择 MAC Addresses 选项，如图 7-39 所示。在右侧栏中，即可根据 MAC 地址来设置要捕获内容，但由于 MAC 地址既难记又难写，通常不使用该过滤器，而是设置要捕获的 IP 地址。

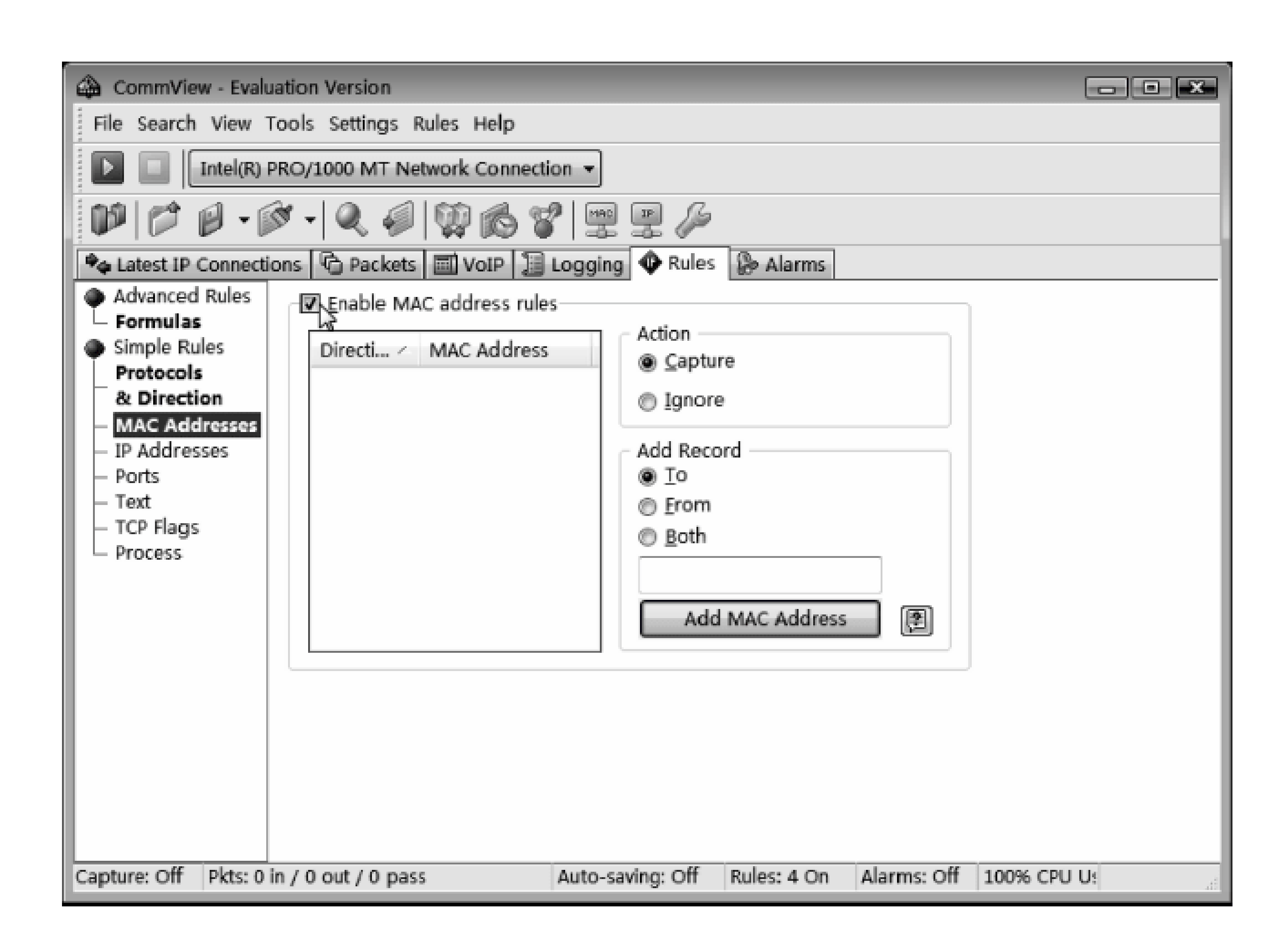


图 7-39　MAC Addresses

③ IP Addresses。在左侧列表中选择 IP Addresses 选项，如图 7-40 所示，在右侧选中 Enable IP address rules 复选框，启用 IP 地址规则。选中 Action 选项区域中的 Capture 单选按钮，在 Add Record 选项区域可设置 IP 规则，To 表示目的地址，From 表示源地址，Both 表示两者都有，例如，要捕获从 192.168.1.100 的计算机发出的数据包，可选中 From 单选按钮，在该文本框中输入 192.168.1.100，单击 Add IP Address 按钮即可添加到左侧的列表框中，CommView 则只捕获从 192.168.1.100 发出的数据包，而不捕获其他数据。按照同样步骤，可以设置多个 IP 地址。

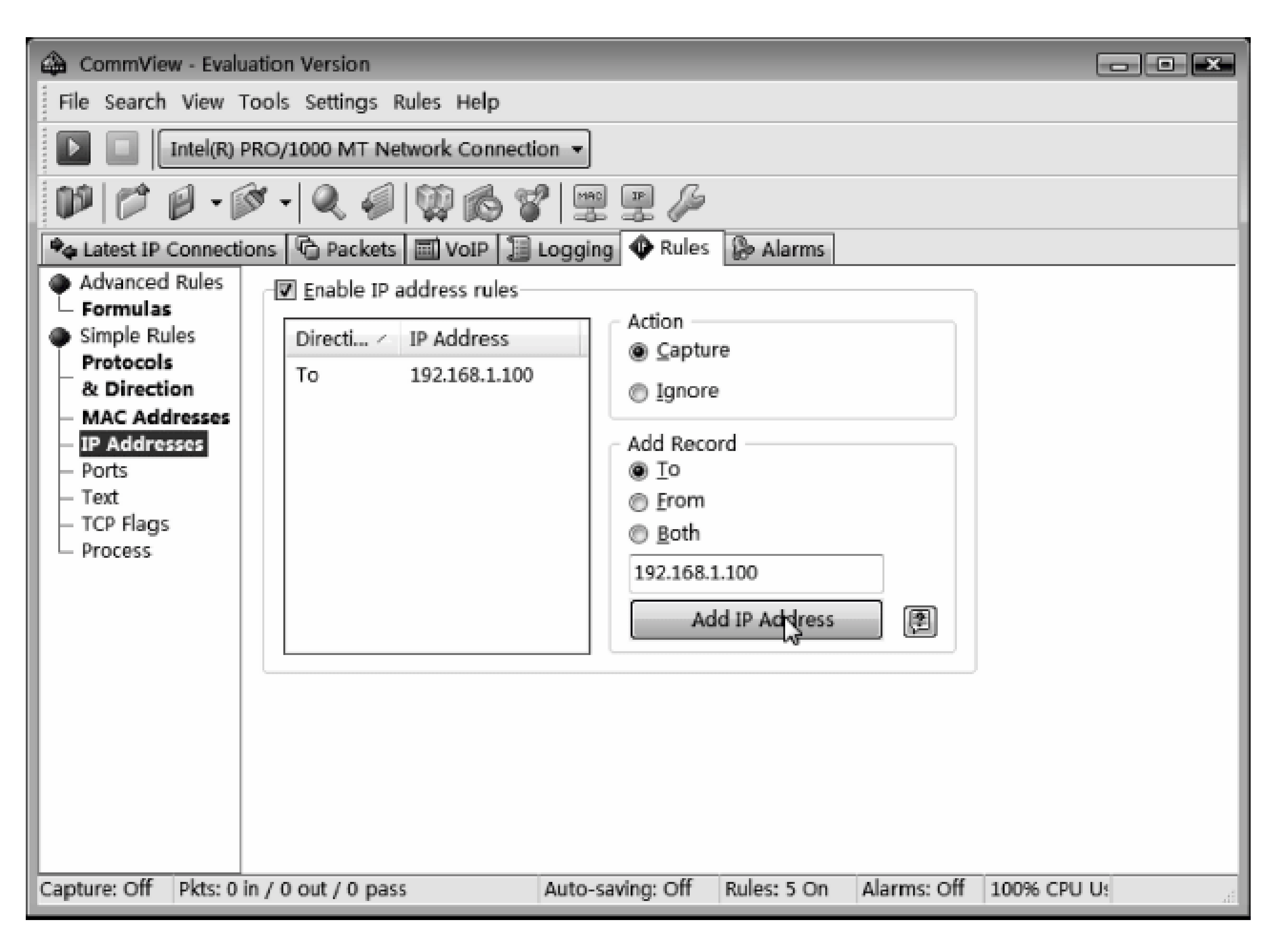


图 7-40 设置 IP 地址规则

④ Ports。在左侧列表中选择 Ports 选项，设置要捕获的端口，如图 7-41 所示。在右侧列表中，选中 Enable port rules 复选框，启用端口规则，选中 Action 选项区域中的 Capture 单选按钮，在 Add Record 选项区域中即可添加要捕获的端口，例如，捕获从 135、445 等端口发出的数据包，可先选中 From 单选按钮，在文本框中输入端口号，单击 Add Port 按钮添加到列表框中，CommView 即可捕获从这些端口传出的数据。

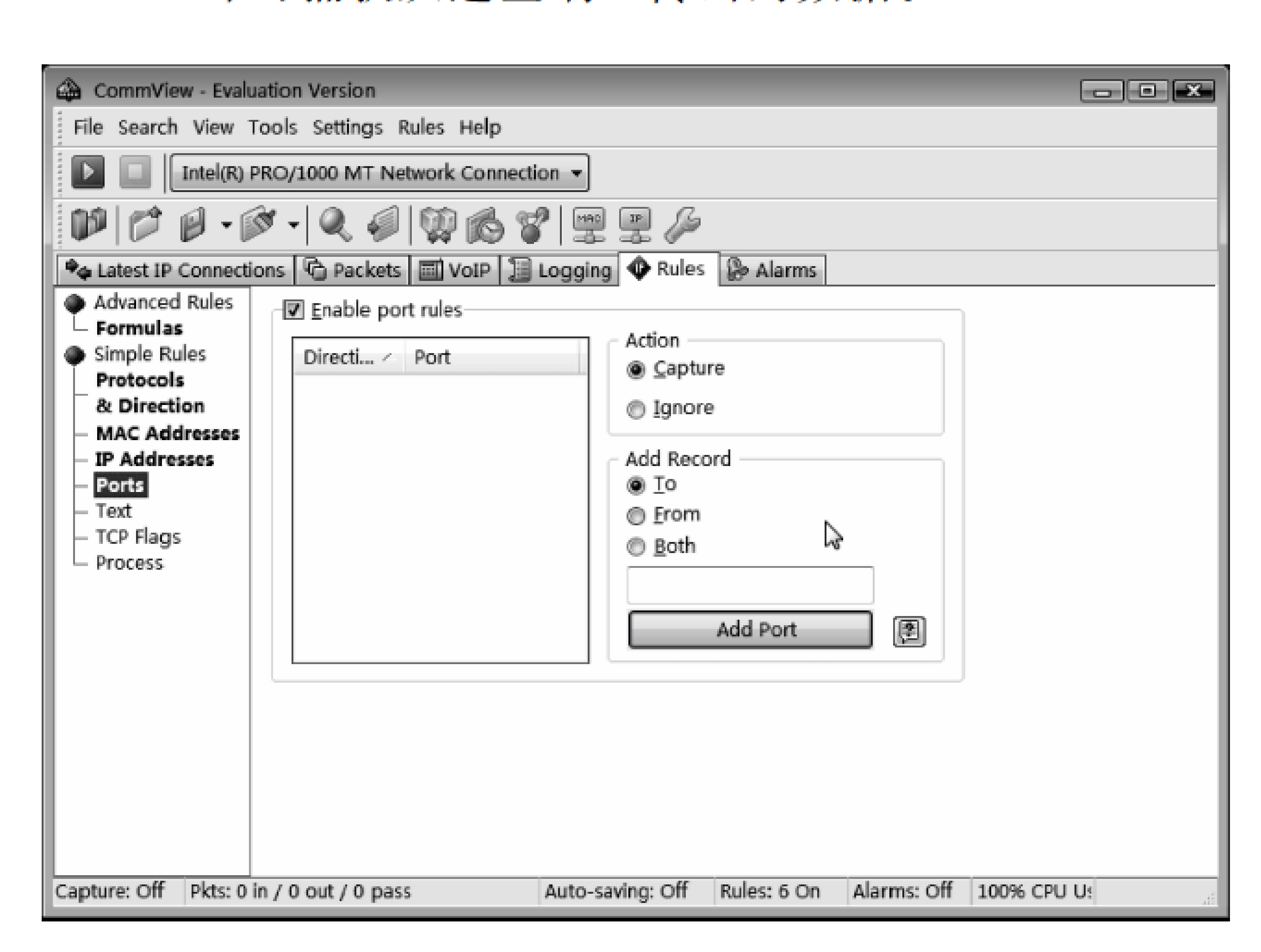


图 7-41 设置端口规则

⑤ Text。在左侧列表中选择 Text 选项，设置捕获具有哪些关键字的数据，如图 7-42 所示。在右侧列表中，选中 Enable text rules 复选框启用该功能，选中 Action 选项区域的 Capture 单选按钮，在 Add Record 选项区域中，即可选择关键字格式。其中，As String 单选按钮表示使用文本格式，As Hex 单选按钮则表示使用 Hex 格式。通常情况下，使用文本格式更容易理解，例如，要捕获网络中 QQ 的传输数据，就可以捕获具有 shenzhen 字样的数据。

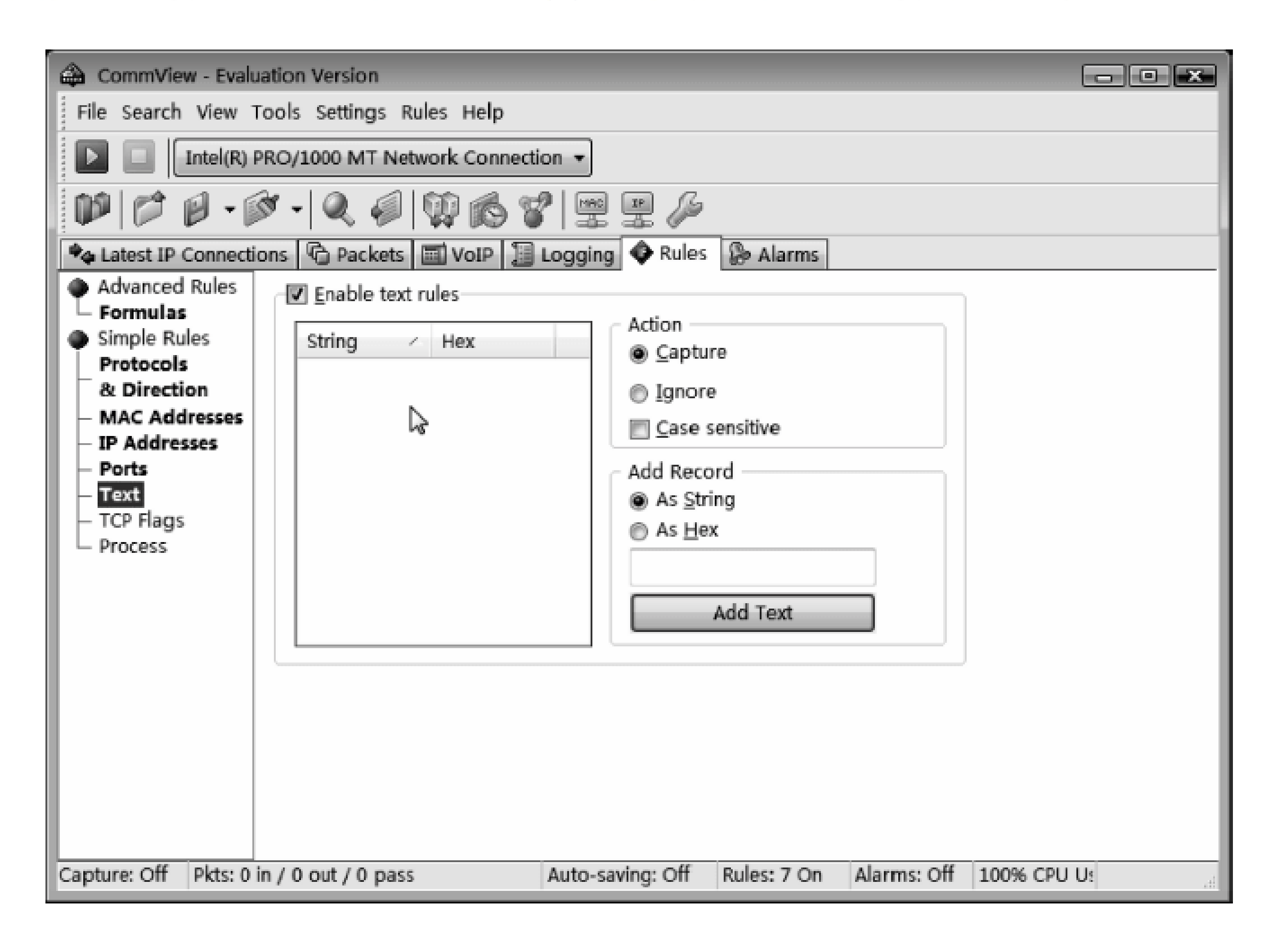


图 7-42 Text 窗口

⑥ TCP Flags。选择左侧列表中的 TCP Flags 选项，设置捕获带有 TCP 标记的数据包，如图 7-43 所示。在右侧列表中，选中 Enable TCP flags rules 复选框，启动 TCP 标记规则，选中 Action 选项区域中的 Capture 单选按钮，然后在 Add Record 选项区域中即可选择要添加的标记，如 FIN、ACK 等。最后，单击 Add Flags 按钮，即可添加到 Flags 列表框中。此时，CommView 在捕获数据时只捕获具有此标记的数据。

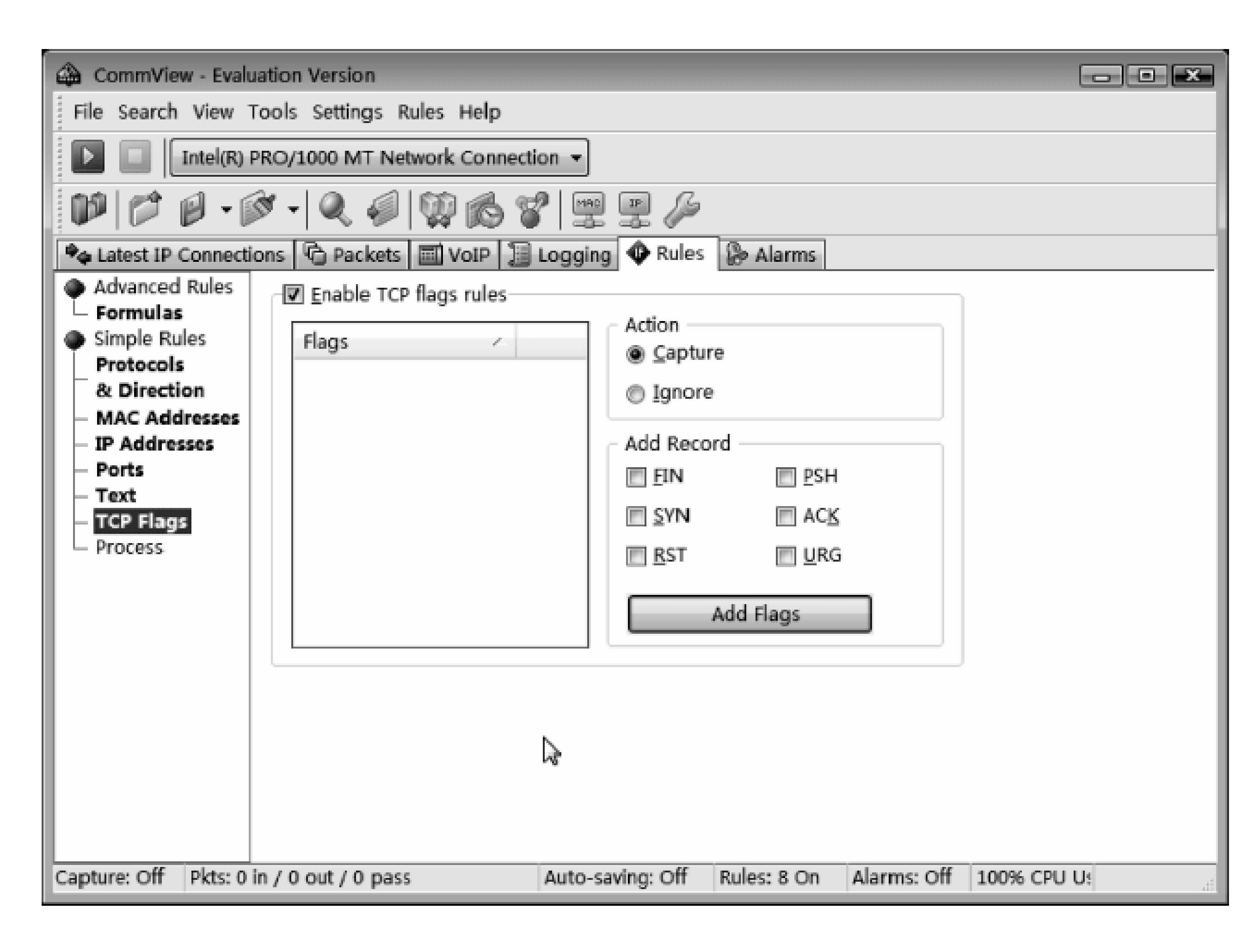


图 7-43 设置 TCP 标记

⑦ Process。允许用户基于处理名称捕获数据包，在左侧列表中选择 Process 选项，如图 7-44 所示。在右侧栏中，选中 Enable Process rules 复选框，启用进程名称捕获数据包。选中 Capture 单选按钮，在 Add Record 文本框中，输入进程名称。单击 Add Process Name 按钮，即可将该进程过滤器添加到列表中。

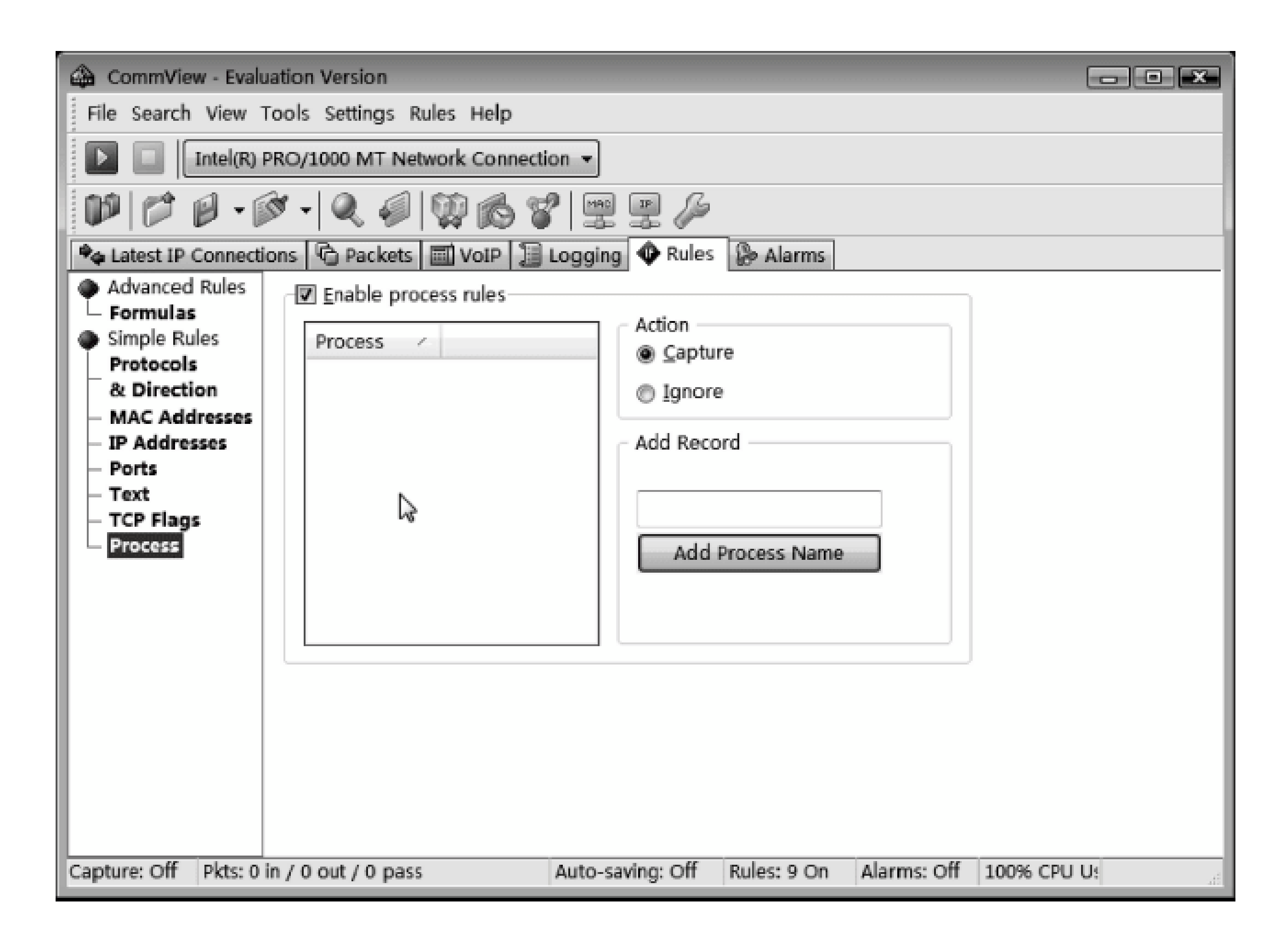


图 7-44 Process

注意：如果哪些规则被启用，则在左侧列表框中，相应的规则名称会以黑体字醒目显示。

（3）保存过滤器

将设置的过滤器进行保存，可以方便以后再次使用。在 CommView 窗口中，依次选择 Rules→Save Current Rules As 命令，根据需要保存过滤器即可。

需要再次使用该过滤器时，可依次选择 Rules→Load Rules From 命令，选择已保存的规则即可。

5. 设置警报

CommView 还可以设置警报，可以将特殊数据包设定为警报信息，当捕获到警报数据包时或未知的 IP 地址时，就会向网络管理员自动发出警报。

（1）在 CommView 窗口中，选择 Alarms 选项卡，显示图 7-45 所示的窗口，首先需要选中 Enable alarms 复选框，启用报警功能。

（2）单击 Add 按钮，添加一个警报，显示图 7-46 所示的 Alarm Setup 对话框。在 General 选项区域的 Name 文本框中为该警报设置一个名称。在 Alarm type 选项区域中选择警报类型，若选中 Packet occurrence(enter a formula)单选按钮，并在该框中设定数据包公式，当捕获到该类数据包时就会自动报警，例如，要将从 4000 端口传出的数据包作为警报，可输入公式 dir=out and dport=4000。对于 Unknown MAC address 和 Unknown IP address 单选按钮，如果选择并单击 Configure 按钮添加允许接收的 MAC 或 IP 地址，当捕获到不在该 MAC 或 IP 地址列表中的地址发送的消息时就会发出警报。

在 Action 选项区域中，可设置的报警方式如下。

① Display message：显示消息。选中该复选框并在该文本框中输入要显示的消息，当报警时就会显示这些字符。

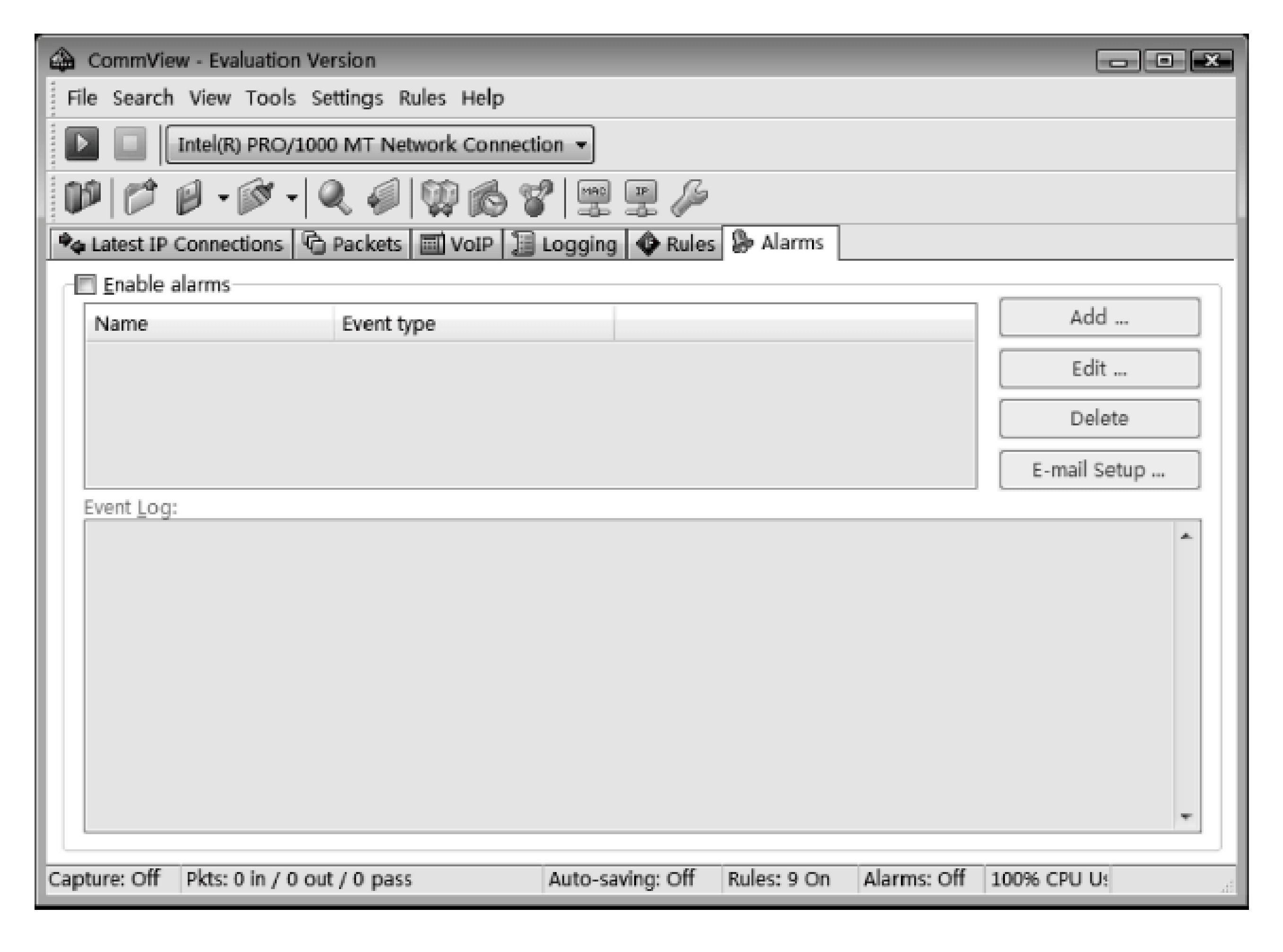


图 7-45　设置警报

② Play sound：声音报警。选中该复选框并输入声音文件所在的路径，当报警时计算机就会自动播放该声音文件来提醒管理员。需要注意的是，只能使用.wav 格式的声音文件。

③ Launch application：运行应用程序。选中该复选框并在该框中输入要运行的应用程序路径，当报警时就会自动运行该程序，例如，可以在报警时运行屏幕保护程序或某个声音、歌曲文件来提醒管理员。

④ Send e-mail to：设置邮件报警，当警报发生时，可以向管理员发送一封邮件。选中 Send e-mail to 复选框，单击 E-mail Setup 按钮，显示图 7-47 所示的对话框，在 Hostname 文本框中输入邮件发送服务器地址，如 smtp.163.com；在 Port 文本框中，使用默认的 25 端口即可。选中 Authentication 复选框，分别在 Username 和 Password 文本框中，输入登录邮件服务器的用户名和密码。在 Your e-mail address(will be used in the"From" field)文本框中输入显示在对方邮箱中的邮件地址，设置完成后单击 OK 按钮，并在 Send e-mail to 框中输入要接收邮件的电子邮箱地址。单击 Test 按钮，可以立即发送一封邮件，测试 E-mail 的设置是否正确。

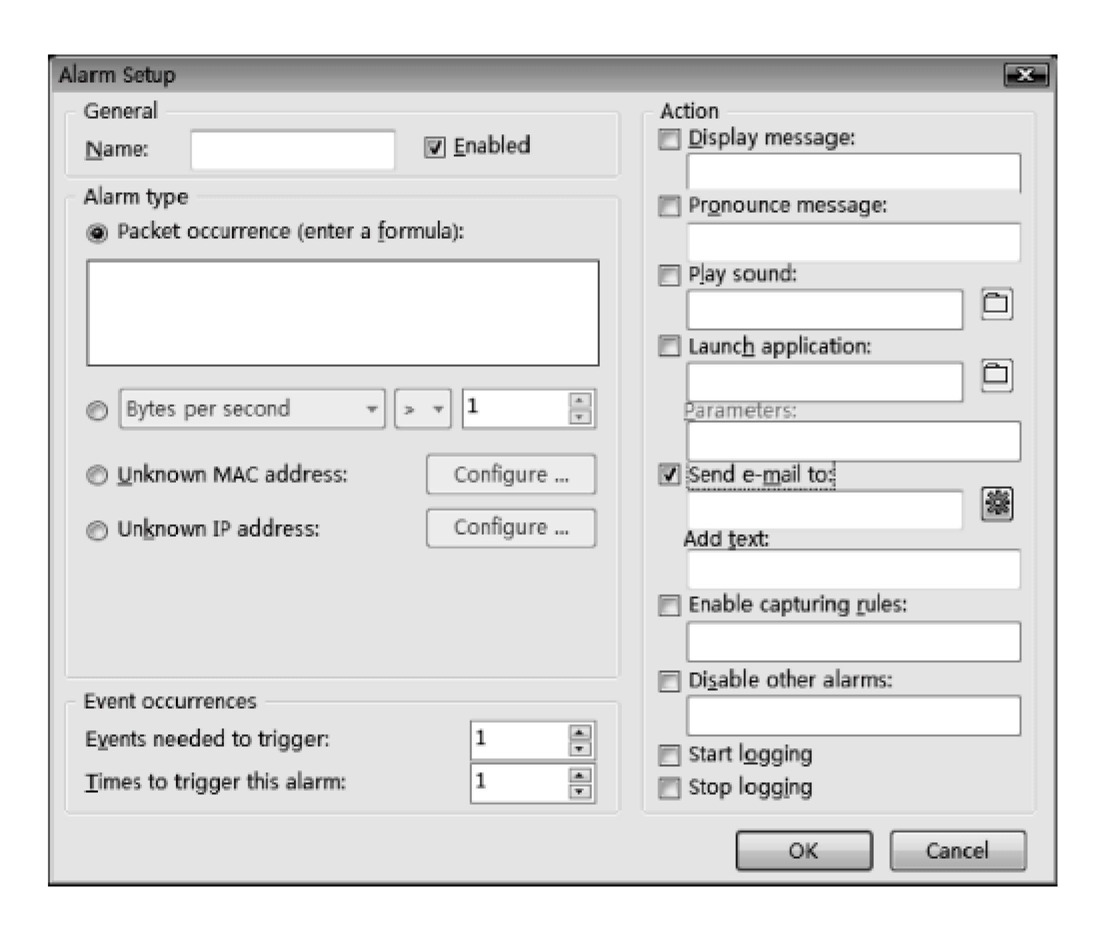


图 7-46　Alarm Setup 对话框



图 7-47　设置 E-mail

⑤ Enable capturing rules：开启捕获规则。

⑥ Disable other alarms：选中该复选框则会关闭其他警报，只使用这一个警报。

⑦ Start logging：选中该复选框，可将报警记录到日志中。

（3）设置完成后，单击 OK 按钮即可。该警报会添加到 CommView 窗口中的 Alarms 选项卡的列表框中。

重复操作可设置多个警报，如果某个警报不想使用，只要取消相应的复选框即可。然后，在 CommView 窗口中运行捕获功能，当捕获到了警报中设置的数据时，即可自动发出警报。

6. 远程监控

CommView 还具有远程监控功能，无论被监控的计算机处于何处，只要连接到 Internet，管理员就可以使用 CommView 远程监控计算机中传输的数据。但首先必须在被监控的计算机上安装 CommView Remote Agent 2.1 插件，才可以实现远程监控，该插件也可从其官方网站（http://www.tamos.com/）上下载。

这里将被监控的计算机称为被控端，监控被控端的计算机称为主控端。

（1）在被控端计算机上安装 CommView Remote Agent 2.1 插件，安装完成后并运行，显示图 7-48 所示的 Remote Agent Configuration and Installation 对话框。需要设置一个端口和密码，供主控端监控被控端时使用。例如，在 Port number 文本框中设置端口号，默认端口号为 5050；在 Password 文本框中，设置一个远程监控密码。

（2）单击 Next 按钮，CommView Remote Agent 开始配置并运行相应的服务，如图 7-49 所示。

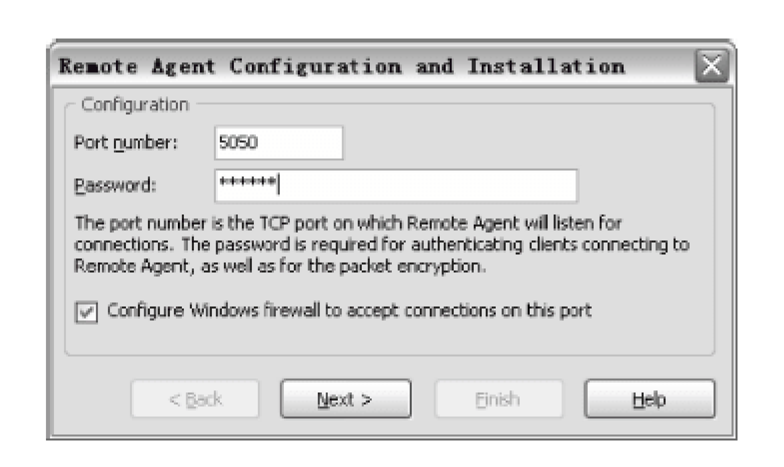


图 7-48　设置端口和密码



图 7-49　配置并运行服务

（3）完成配置后，单击 Finish 按钮，即可完成被控端的设置。

（4）在主控端计算机上，依次选择 File→Remote Monitoring Mode（远程监控模式）命令，显示图 7-50 所示的窗口。

（5）单击 New Remote Agent Connection 按钮，显示图 7-51 所示的 Remote Agent Connection 窗口。在 Host or IP address 文本框中，输入要监控的计算机 IP 地址，如 192.168.1.190。在 Password 文本框中，输入在远程计算机上安装 CommView Remote Agent 时所设置的密码。

（6）单击窗口上方的 Connect 按钮，开始连接远程计算机，连接成功以后会在 Adapter 下拉列表框中显示出远程计算机上所有的网络连接，在该下拉列表框中选择一个合适的网络适配器，如图 7-52 所示。

（7）单击 Start Capture 按钮，CommView Remote Agent 即可在远程计算机上捕获到数



图 7-50　远程监控模式

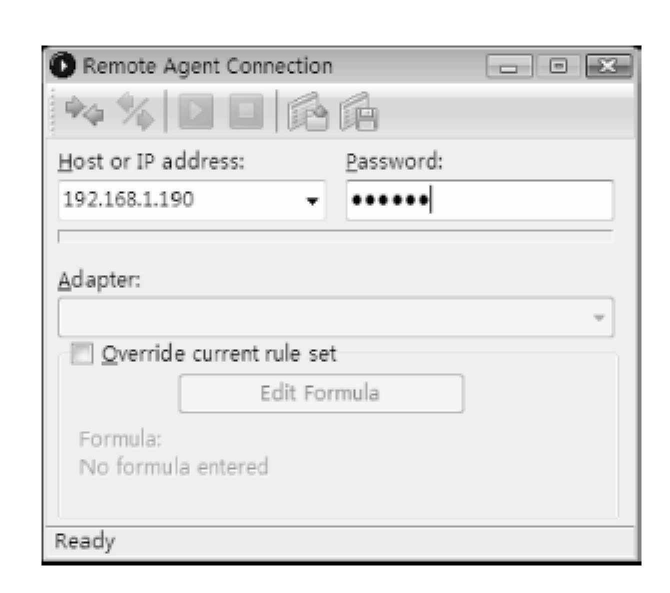


图 7-51　Remote Agent Connection 窗口

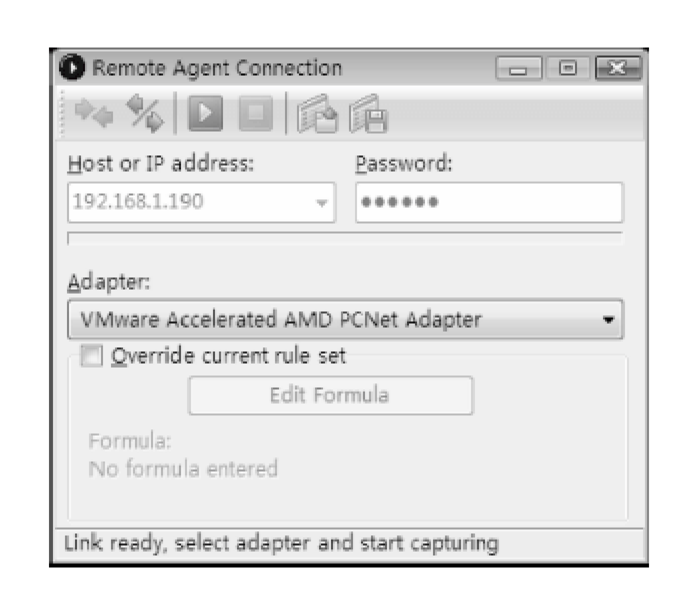


图 7-52　连接远程计算机

据包，并显示在 CommView 窗口中，网络管理员就可以根据所监控的信息，远程分析网络状况了，如图 7-53 所示。

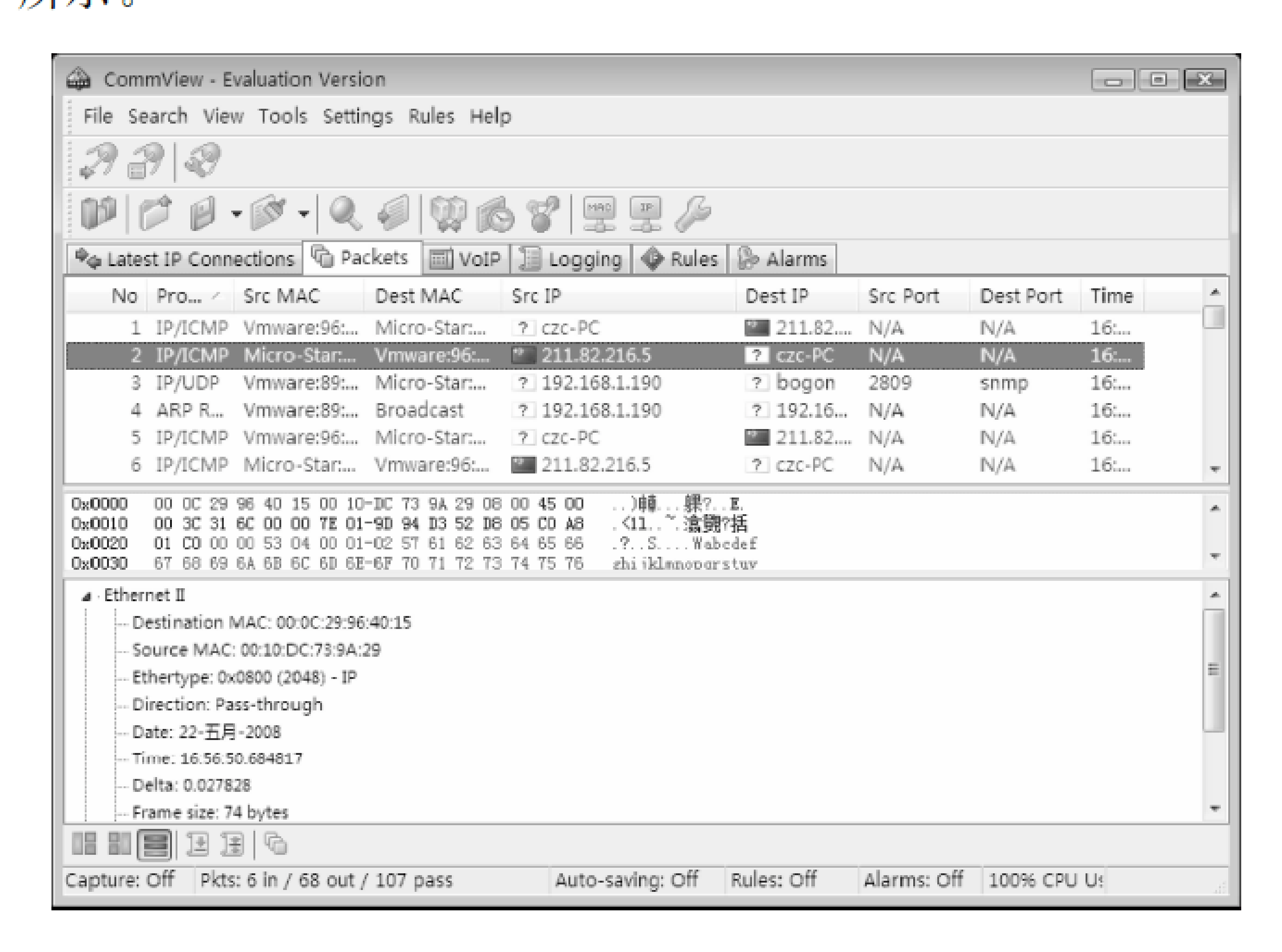
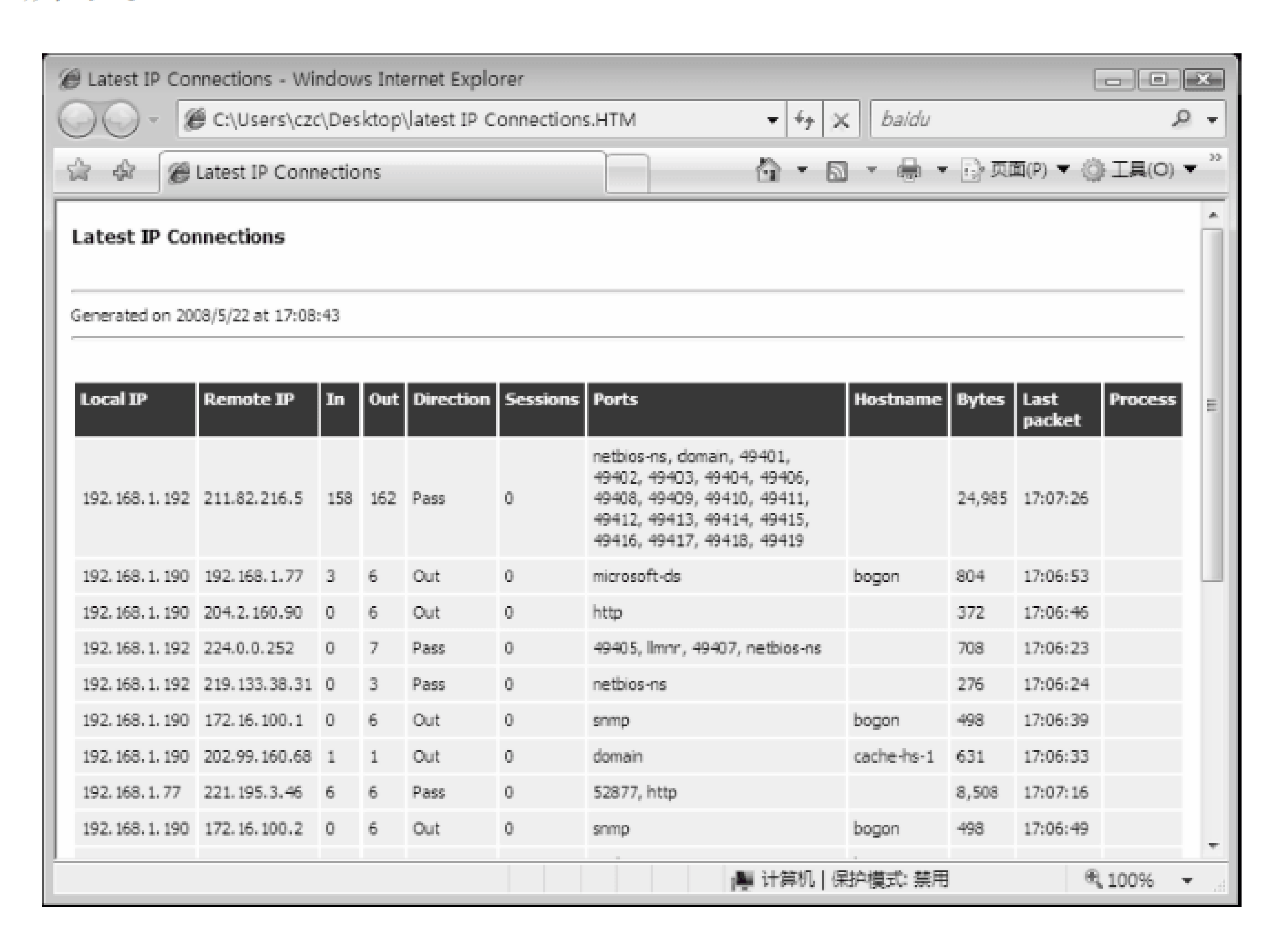


图 7-53　捕获远程计算机数据包

7. 保存捕获数据

当数据捕获完成以后，为便于网络管理员以后再进行查看分析，可以将这些数据保存起来。CommView 捕获的数据可以保存成.htm 格式或.csv 格式。

在 CommView 窗口中，依次选择 File→Save latest IP Connections As 命令，将当前数据保存起来即可，并保存成网页表格形式。如果日后想查看相关信息，直接打开保存的网页即可，如图 7-54 所示。



Latest IP Connections

Generated on 2008/5/22 at 17:08:43

Local IP	Remote IP	In	Out	Direction	Sessions	Ports	Hostname	Bytes	Last packet	Process
192.168.1.192	211.82.216.5	158	162	Pass	0	netbios-ns, domain, 49401, 49402, 49403, 49404, 49406, 49408, 49409, 49410, 49411, 49412, 49413, 49414, 49415, 49416, 49417, 49418, 49419		24,985	17:07:26	
192.168.1.190	192.168.1.77	3	6	Out	0	microsoft-ds	bogon	804	17:06:53	
192.168.1.190	204.2.160.90	0	6	Out	0	http		372	17:06:46	
192.168.1.192	224.0.0.252	0	7	Pass	0	49405, llmnr, 49407, netbios-ns		708	17:06:23	
192.168.1.192	219.133.38.31	0	3	Pass	0	netbios-ns		276	17:06:24	
192.168.1.190	172.16.100.1	0	6	Out	0	snmp	bogon	498	17:06:39	
192.168.1.190	202.99.160.68	1	1	Out	0	domain	cache-hs-1	631	17:06:33	
192.168.1.77	221.195.3.46	6	6	Pass	0	52877, http		8,508	17:07:16	
192.168.1.190	172.16.100.2	0	6	Out	0	snmp	bogon	498	17:06:49	

图 7-54 查看保存的数据

7.3.2 网络流量实时监控——MRTG

MRTG 是一款非常有名的网络流量监视及统计软件，MRTG 可以以网页及图形的方式来呈现出目前网络流量的状况。网络中安装了 MRTG 后，管理员可以及时了解服务器和交换机的流量，防止因流量过大而导致服务器瘫痪或网络拥塞。

1. MRTG 简介

MRTG(Multi Router Traffic Grapher，MRTG)是一款监控网络链路流量负载的工具软件，通过 SNMP 协议从设备得到设备的流量信息，并将流量负载以包含 png 格式图形的 HTML 文档方式显示给用户，以非常直观的形式显示流量负载。

作为目前最为通用的网络流量监控软件，MRTG 具有以下特点。

(1) 可移植性：可以运行在大多数 Linux/UNIX 系统和 Windows 2000/XP/2003 系统。

(2) 源码开放：MRTG 是用 Perl 编写的，源代码完全开放。

(3) 高可移植性的 SNMP 支持：MRTG 采用了 Simon Leinen 编写的具有高可移植性的 SNMP 实现模块，从而不依赖于操作系统的 SNMP 模块支持。

(4) 支持 SNMPv2c：MRTG 可以读取 SNMPv2c 的 64 位的计数器，从而大大减少了计数器回转次数。

(5) 可靠的接口标识：被监控设备的接口可以以 IP 地址、设备描述、SNMP 对接口的编号及 MAC 地址来标识。

(6) 常量大小的日志文件：MRTG 的日志不会变大，因为这里使用了独特的数据合并

算法。

（7）自动配置功能：MRTG 自身有配置工具套件，使得配置过程非常简单。

（8）性能：时间敏感的部分使用 C 代码编写，因此具有很好的性能。

（9）png 格式图形：图形采用 GD 库直接产生 png 格式。

（10）可定制性：MRTG 产生的 Web 页面是完全可以定制的。

2. 网络设备和服务器的准备

这里服务器使用的操作系统为 Windows Server 2003，以管理网络中的 Cisco 交换机为例进行介绍。

（1）安装 Web 服务

在监控计算机上安装并启用 Web 服务，具体安装步骤可参见相关内容，这里就不再赘述。

（2）安装 ActivePerl

在监控计算机上下载并安装 Windows 版本的 Perl 编译程序。由于 MRTG 是使用 Perl 语言编写的，所以，在 Windows 环境中需要先来配置 Perl 环境。Perl 可以从其官方网站（http://www.activestate.com/）免费下载。ActivePerl 安装过程非常简单，建议采用系统安装默认值，一般安装在 C:\Perl 目录下，并在系统环境变量 PATH 中加入 C:\Perl\bin。

小知识： ActivePerl 是 Windows 系统环境下的 Perl 语言解释器的源代码，支持 Microsoft IIS，包括有 Perl for Win32、Perl for ISAPI、PerlScript、PerlPackageManager 共 4 套程序。

（3）启用服务器上的 SNMP 服务

若欲借助网络管理软件实现对网络设备和服务器的远程管理与监视，必须在网络设备和服务器上启用 SNMP 服务。具体操作内容可参见相关内容，这里就不再赘述。

（4）配置网络设备的 SNMP 服务

下面以 Cisco 为例，介绍一下如何启用网络设备的 SNMP 服务。

① 为网络设备配置管理 IP 地址。

```
Switch>enable
Password:
Switch#
Switch# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# ip address 管理 IP 地址 子网掩码
Switch(config-if)# no shuwdown
Switch(config-if)# end
Switch# write memory
```

② 启用 SNMP 服务。

```
Switch>enable
Password:
Switch#
```

```
Switch# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#
Switch(config)#snmp-server community public RO /只读字符串为 public
Switch(config)#snmp-server community private RW /读写字符串为 private
Switch(config)#snmp-server enable traps
Switch(config)# snmp-server host ip_address SNMP_hostname /安装 MRTG 的计算机的 IP 地址
Switch(config)#exit
Switch# write memory
```

(5) 监控服务器设置

如果想要监控网络中的服务器,则需要在目标服务器安装简单网络管理协议。具体安装并启用 SNMP 的操作,参见本书的相关内容,这里就不再赘述。

3. 监控计算机上的 MRTG 配置

对服务器和交换机的监控的配置基本相同。这里以对服务器的监控为例。欲监测的设备是 Web 服务器,其 SNMP 监控的 IP 地址是 192.168.1.10,SNMP 查询字符串为 public。

(1) 下载 Windows 版本的 MRTG 并安装。

(2) 配置 Web 服务器,并配置 MRTG 生成结果页面的文件夹。

① 将 D:\web\MRTG 作为存放被采集设备配置文件的文件夹。

② 将 D:\web\MRTG\Web 作为存放被采集信息文件(HTML 与图片)的文件夹。

③ 配置 Web 服务器,建立一个虚拟目录 http://localhost/MRTG/作为查看 MRTG 结果的路径,并指向到 D:\web\MRTG。

(3) 生成 Web 服务器的 MRTG 采集配置文件。

在 MS-DOS 窗口 C:\MRTG\bin\提示符下运行以下命令。

```
Perl cfgmaker --global "WorkDir: d:\web\MRTG\Web" --output "d:\web\MRTG\Web.cfg" pub@
192.168.1.10
```

如果运行正常将会在 D:\web\MRTG\目录生成 cisco4006.cfg 文件,这个就是针对 Web 的 MRTG 配置文件。

(4) 修改 Web 服务器的 MRTG 采集配置文件。

使用文本编辑器打开 D:\web\MRTG\web.cfg 文件进行编辑,在其中加入如下语句。

```
RunAsDaemon: yes
```

表示允许程序及配置文件后台运行。

```
Options[_]: growright, bits
```

表示采集的流量信息使用 bits 进行表示,也可以使用 bytes 进行表示。

```
Languagd: GB2312
```

表示使用中文生成 MRTG 结果信息文件。

(5) 运行 MRTG 流量采集程序。

在 MS-DOS 窗口运行以下命令。

```
c:\MRTG\bin\> start /D c:\MRTG\bin wPerl MRTG --logging=eventlog d:\web\MRTG\
web.cfg
```

如果运行正常将会在 D:\web\MRTG 目录生成 web.cfg_l 文件，并在 D:\web\MRTG\web 目录生成 MRTG 第一次采集生成的大量结果文件，可以通过 Web 浏览器进行查看，地址为：http://localhost/MRTG/Web/。

同时可以观察到系统将会每 5 分钟自动运行一次 MRTG，采集流量信息并生成文件。

(6) 生成 Web 索引页面。

在 MS-DOS 窗口运行以下命令。

```
c:\MRTG\bin\ Perl indexmaker --output="d:\web\MRTG\web\index.html" --title=
windowMRTG d:\web\MRTG\web.cfg
```

如果运行正常将会在 d:\web\MRTG\web 目录生成 index.html 页面，通过 Web 浏览器查看，地址为："http://localhost/MRTG/web/index.html"。图 7-55 所示为服务器性能信息与流量信息索引图。



图 7-55　服务器性能信息与流量信息索引图

当欲监视的设备为交换机时，可以通过修改.cfg 中每个端口的 Title、PageTop 信息来指定每个端口流量信息页面的标题，也可以修改.cfg 中其他的一些信息，或者修改 index.html 文件来改变页面的显示。图 7-56 所示为网络设备流量监控图。

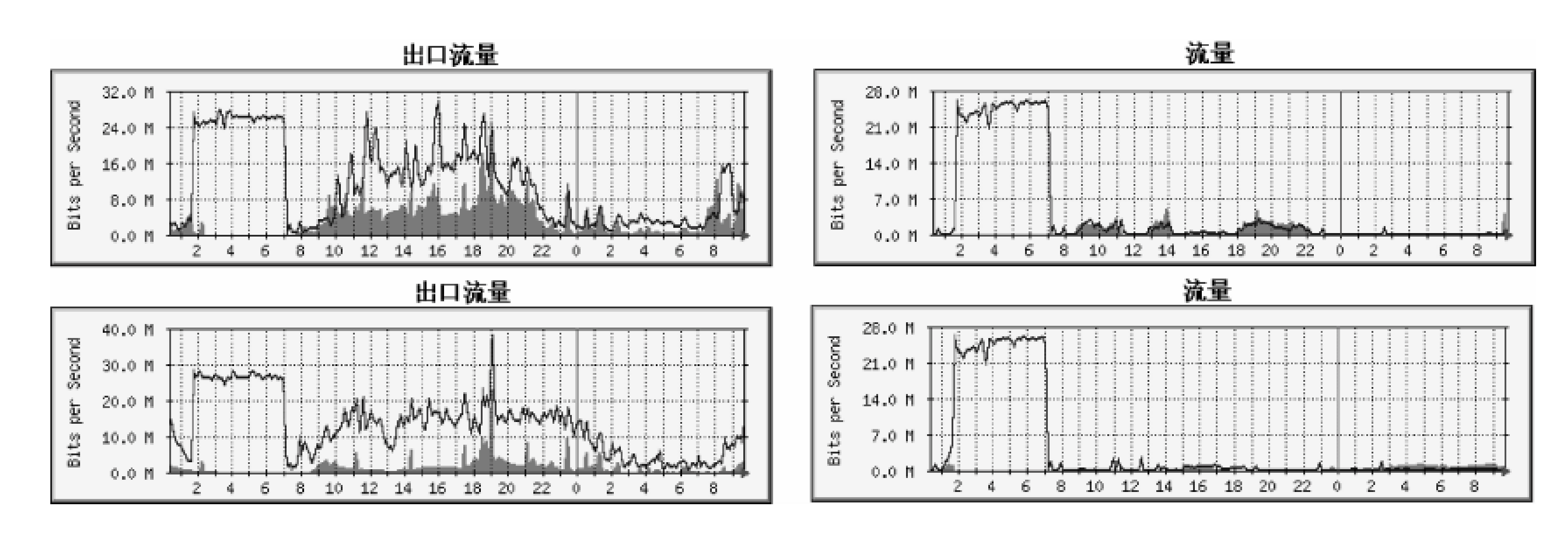


图 7-56　网络设备流量

7.4 网络吞吐量分析

网络性能是衡量网络布线系统和网络设备系统的基本因素，换句话说，所有的网络在规划、施工以及日常维护都是为了保证网络性能而展开的。因此，测试网络性能是网络的重要工作之一。不仅在网络建设完成后需要测试网络性能，在日常管理中，也应时常进行网络性能的测试，这样可以排除某些网络故障。

7.4.1 吞吐率测试——Qcheck

Qcheck 是 NetIQ 公司开发的一款免费网络测试软件，被 NetIQ 称为“Ping 命令的扩展版本”，主要用来测试网络的响应时间和数据传输速率。Qcheck 可以运行于所有 Windows 9x 以后的操作系统上。

1. Qcheck 的运行

Qcheck 的运行需要两台计算机，并分别安装 Qcheck。当进行测试时，只需要从一台客户端计算机向另一端计算机发送文件或测试命令即可，例如 TCP/UDP 传输速率测试。测试结果越高越好，100Mbps 端口的理论值最高为 94Mbps(传输速率)。

(1) 在要测试的网络两端分别运行 Qcheck 程序，显示图 7-57 所示的 Qcheck 主界面。



图 7-57　Qcheck 主界面

(2) 在 Qcheck 主界面上方的 From Endpoint 1 下拉列表框中输入要发送数据的端点；在 To Endpoint 2 下拉列表框中输入要将数据发送到的端点。下面有几个圆按钮，左侧的 Protocol 选项区域内的按钮表示可以使用的协议类型，包括 TCP、UDP、SPX 和 IPX。右侧的 Options 选项区域内的按钮表示可以测试的项目。根据所选择项目的不同，所适用的协议也有所不同。

① Response Time(响应时间)：测试响应的最短、平均与最长时间。适用于所有的协议。

② Throughput(吞吐量)：测试在每秒送出的数据量，以测试网络带宽。适用于所有的协议。

③ Streaming：测试串流传输速率，如多媒体流的带宽。只适用于 UDP 和 IPX 协议。

④ Traceroute：Traceroute 与 Windows 中的 Tracert 命令作用相同，测试一台计算机到另一台计算机所经过的路由。只适用于 TCP 和 UDP 协议。

(3) 单击 Run 按钮即可开始测试，测试完成以后会在下面的黑色框中显示出测试结果，也可以单击 Details 按钮查看详细信息。

2. 测试 TCP 响应时间

TCP 响应时间(TCP Response Time)测试可以测试出完成 TCP 通信的最短、平均与最长时间等信息。

(1) 运行 Qcheck，在 From Endpoint 1 下拉列表框中选择 localhost 选项，即从本地计

算机发送测试命令，在 To Endpoint 2 文本框中，输入目标计算机 IP 地址。在 Protocol 选项区域中单击选中 TCP 按钮，在 Options 选项区域中单击选中 Response Time 按钮。在 Iterations 文本框中输入重复测试的次数，默认为 3 次。在 Date Size 文本框中输入要发送的数据包的大小，默认为 100bytes。

（2）设置完成后，单击 Run 按钮，即可开始测试，测试完成后，在 Response Time Results 文本框中显示出测试结果，如 Minimum（最短）、Average（平均）与 Maximum（最长）时间，如图 7-58 所示。

如果想查看更详细的信息，可单击 Details 按钮，打开图 7-59 所示的 Qcheck Results 窗口。在该窗口中显示了设置信息、测试结果，甚至显示了本地计算机与目标计算机的系统信息以及 Qcheck 的版本信息等。在 Response Time Results 选项区域中显示了响应的最小、最大和平均时间。

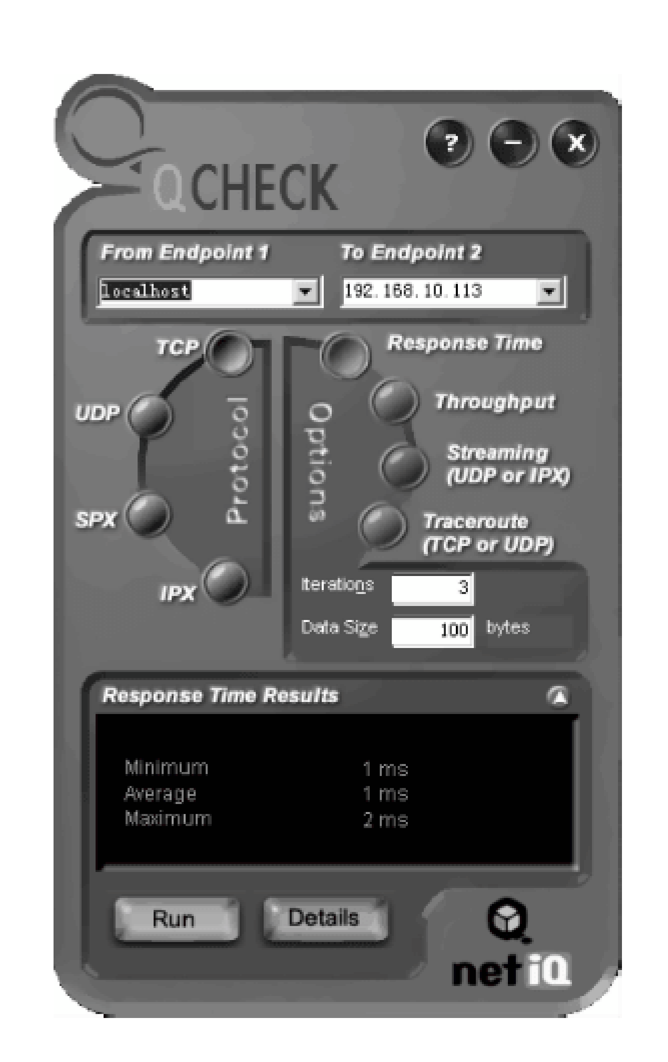


图 7-58　测试 TCP 响应时间

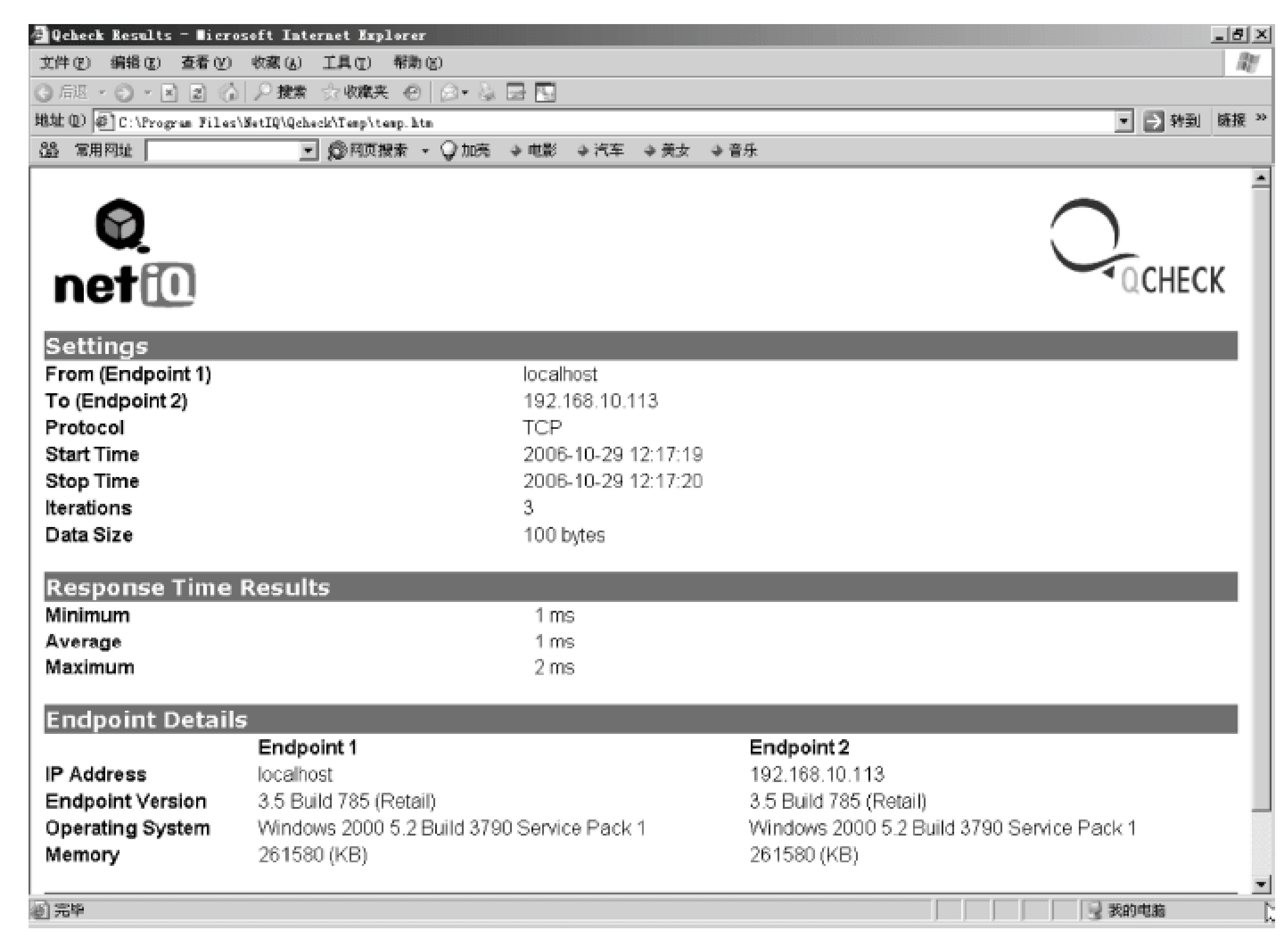


图 7-59　Qcheck Results

3. 测试网络带宽

Qcheck 是一款集网络性能测试和网络带宽测试于一身的软件，不但可以用来测试网络性能，还可以用来测试网络带宽。

（1）运行 Qcheck，在 From Endpoint 1 文本框中选择 localhost；在 To Endpoint 2 文本框中输入目标计算机 IP 地址；在 Protocol 选项区域中单击选择 TCP 按钮，在 Options 选项区域中单击选择 Throughput 按钮；Date Size 文本框中输入要发送的数据包的大小，默认为 100KB。

（2）设置完成后单击 Run 按钮，即可开始测试，测试完成后即在 Throughput Results 文本框中显示测试结果，如图 7-60 所示。

小技巧：在测试网络带宽时，往往会因为设备性能、线路质量等各种因素的影响，使得测试值比实际值要小。为了求得准备的结果，建议使用多台计算机进行测试，一般最大值才是网络带宽的真实值。

4. 串流测试

使用 Qcheck 的 UDP 串流传输速率(UDP Streaming Throughput)测试,可以测试多媒体流通需要多少的频宽,以方便网络硬件速度和网络所能达到真正数据传输速率间的比较。

(1) 运行 Qcheck,在 From Endpoint 1 下拉列表框中选择 localhost 选项;在 To Endpoint 2 下拉列表框中输入目标计算机 IP 地址;在 Protocol 选项区域中单击选中 UDP 按钮,在 Options 选项区域中选中 Streaming 按钮;在 Data Rate 设置数据传输速率,默认为 50kbps,最大不能超过 1Mbps;在 Duration 框中设置持续时间,默认为 10 秒。

(2) 设置完成后单击 Run 按钮,即可开始测试,测试完成以后在 Streaming Results 文本框中显示出测试结果,如图 7-61 所示。这里测试出的传输速率为 49.940kbps。



图 7-60 测试网络带宽

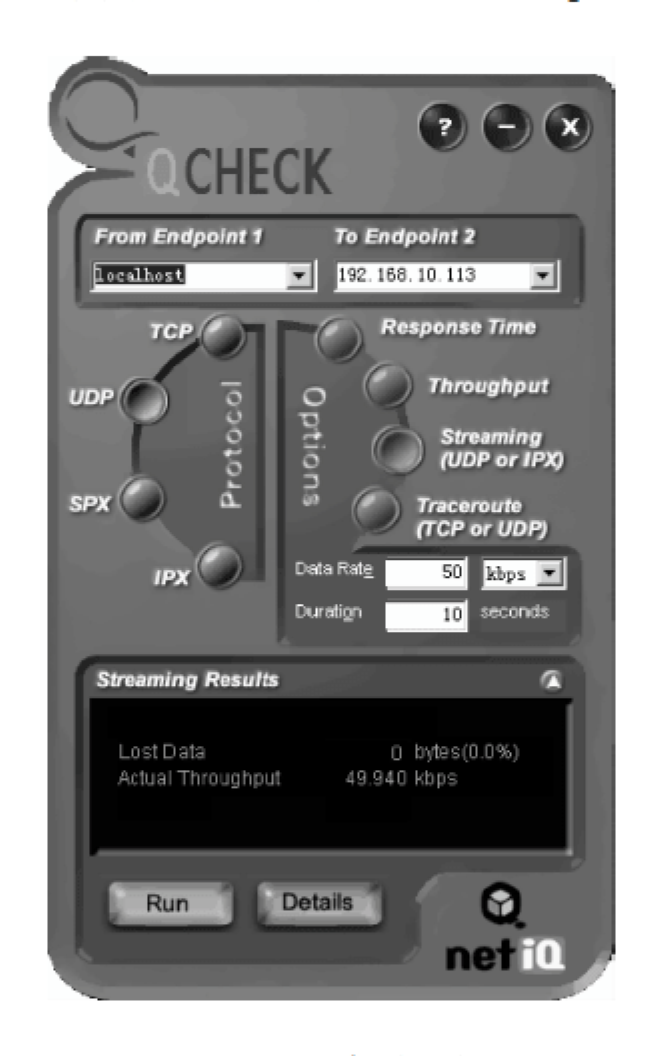


图 7-61 串流测试

7.4.2 SolarWinds

SolarWinds Engineer's Toolset 是一款完善的网络带宽、性能和故障管理软件。可以通过浏览器即时监控网络状态和统计资料。程序将监视和搜集来自路由器、节点、服务器和所有开启 SNMP 服务的设备的信息;同时也将监控本机的 CPU 占用率、内存使用情况以及可用磁盘空间。

1. SolarWinds Engineer's Toolset 简介

SolarWinds Engineer's Toolset 网络性能监视器提供了一个全面的容错和性能管理的平台,可以从 Web 浏览器收集并查看可用性和实时的历史统计信息。监视、收集和成功地分析数据从路由器、交换机、防火墙、服务器和任何其他启用 SNMP 的设备上传输的相关信息,Orion NPM 提供易于使用、可缩放的网络,为 IT 专业人员处理任何大小网络的监视问题。

SolarWinds Engineer's Toolset 提供以下详细监视功能。

(1) 网络的可用性。

(2) 带宽容量使用率。

(3) 缓冲区使用情况和错误。

（4）CPU 和内存利用率。

（5）接口错误和丢弃。

（6）网络延迟。

（7）节点、接口和卷状态。

（8）卷使用情况。

这些监视功能，以及使用完全自定义基于 Web 的界面，警报、报告引擎和灵活的扩展能力帮助 SolarWinds Engineer's Toolset 做出需要进行涉及网络需要最简单的选择。

它的安装需求如下。

（1）使用 32 位或 64 位 Windows 2003 Server 操作系统。

（2）CPU 频率大于 500MHz。

（3）128MB 以上内存。

（4）安装.NET Framework 2.0 以上版本。

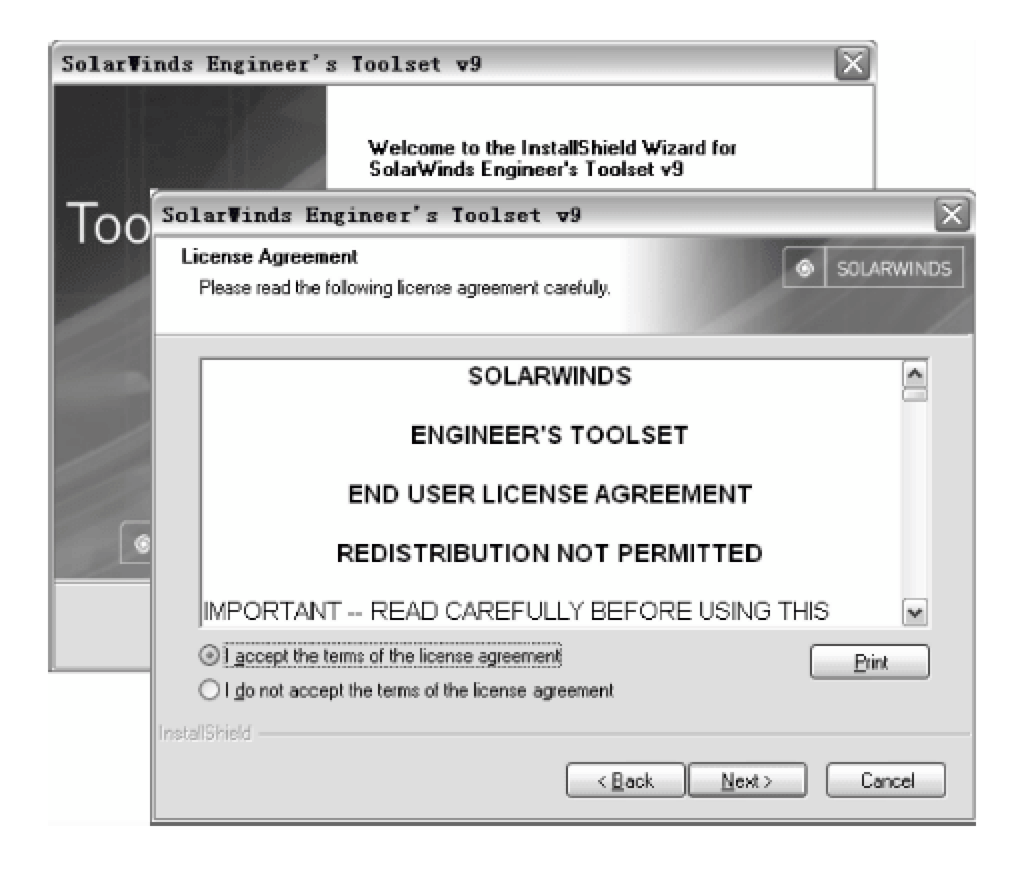
（5）安装 IE6.0 以上版本浏览器。

2. 安装与运行 SolarWinds

SolarWinds Engineer's Toolset 软件可以从其官方网站进行下载，其下载地址为 http://www.solarwinds.com。下载完成后，可按如下步骤安装。

（1）双击安装程序，运行 SolarWinds Engineer's Toolset 安装向导。单击 Next 按钮，显示图 7-62 所示的 License Agreement 对话框。选中 I accept the terms of the license agreement 单选按钮，接受该许可协议。

（2）单击 Next 按钮，显示图 7-63 所示的 Customer Information 对话框。在 User Name 和 Company Name 文本框中，分别输入用户名称和公司名称。如果选中 Anyone who uses this computer(all users)单选按钮，可以使该计算机上的所有用户均可使用该软件，如果选中 Only for my(czc)单选按钮，则仅该用户可以使用该软件。



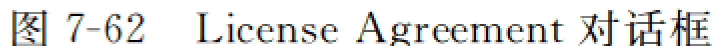


图 7-62　License Agreement 对话框



图 7-63　Customer Information 对话框

（3）单击 Next 按钮，显示图 7-64 所示的 Choose Destination Location 对话框。在该对话框中，可以根据需要设置软件的安装目录，单击 Browse 按钮进行设置即可。

（4）单击 Next 按钮，显示图 7-65 所示的 Ready to Install the Program 对话框。

（5）单击 Install 按钮，即可开始安装软件，安装完成后，显示图 7-66 所示的 SolarWinds

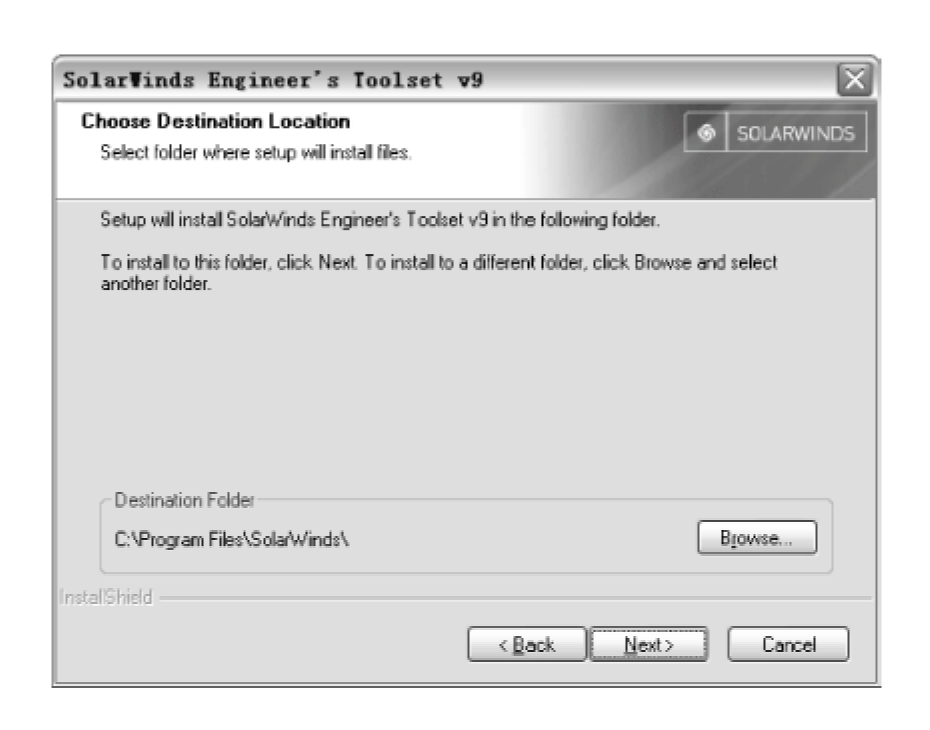




图 7-64 Choose Destination Location 对话框

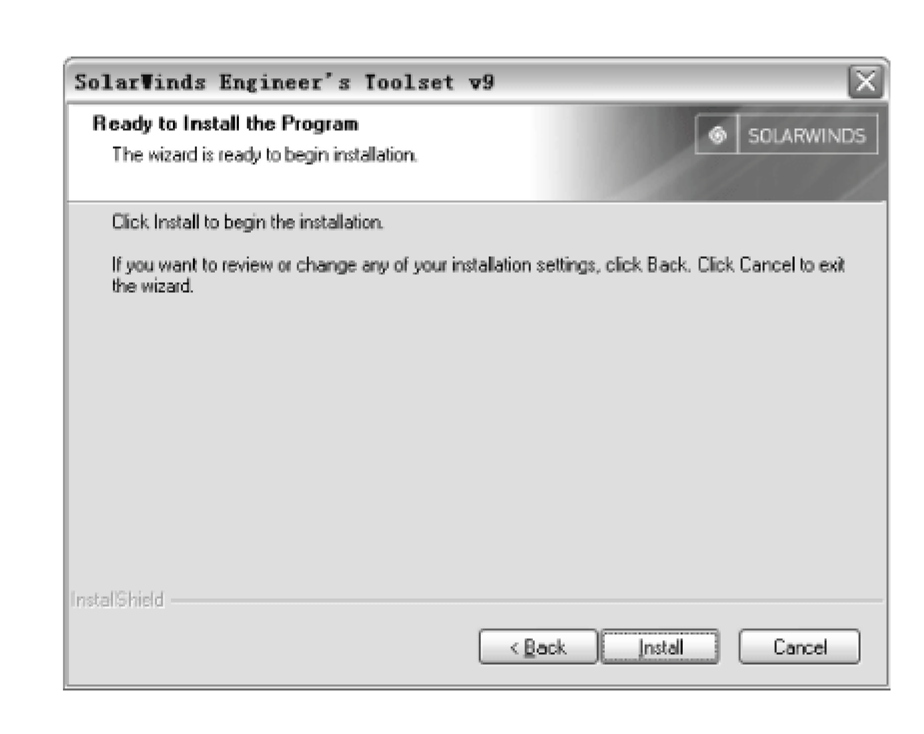


图 7-65 Ready to Install the Program 对话框

Network Management Tools 对话框。根据用户所获得的许可信息，输入相应的文本框中，单击 Continue 按钮即可。如果没有获得许可信息，可单击 Skip This and Enter Software License Key Now 按钮，跳过该操作并输入许可信息。

（6）这里单击 Skip This and Enter Software License Key Now 按钮，跳过该操作，显示图 7-67 所示的 Install Software License Key 对话框。在 Enter Software License Key 文本框中，输入所获得的许可信息。



图 7-66 SolarWinds Network Management Tools 对话框



图 7-67 Install Software License Key 对话框

（7）单击 Continue 按钮，显示图 7-68 所示的成功安装许可证对话框。

（8）单击 Continue 按钮，显示图 7-69 所示的 InstallShield Wizard Complete 对话框。提示需要重新启动计算机，才可以使软件生效。

（9）单击 Finish 按钮，完成安装并重新启动计算机。重新启动计算机后，软件会自动运行，显示图 7-70 所示的软件主窗口。如果软件没有自动运行，可以依次选择"开始"→"所有程序"→SolarWinds Engineer's Toolset→SolarWinds Toolset Launchpad 命令，运行该软件。

3. 发现网络

IP Network Browser 是一个互动的网络发现工具，提供能够扫描 IP 地址范围或子网和显示发现设备包括系统 MIB、ARP 表、接口、IOS、驱动器、Flash 内存等的详细信息。

（1）在软件主窗口左侧栏中，选择 Network Discovery 选项，显示图 7-71 所示的 Network Discovery 窗口。



图 7-68　成功安装许可证



图 7-69　InstallShield Wizard Complete 对话框

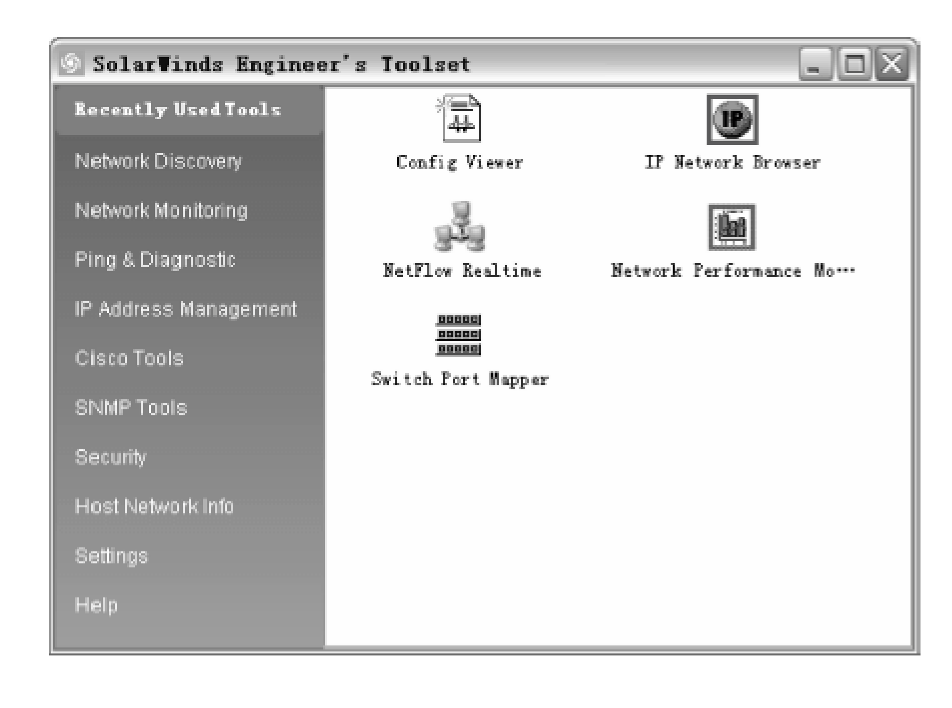


图 7-70　软件主窗口

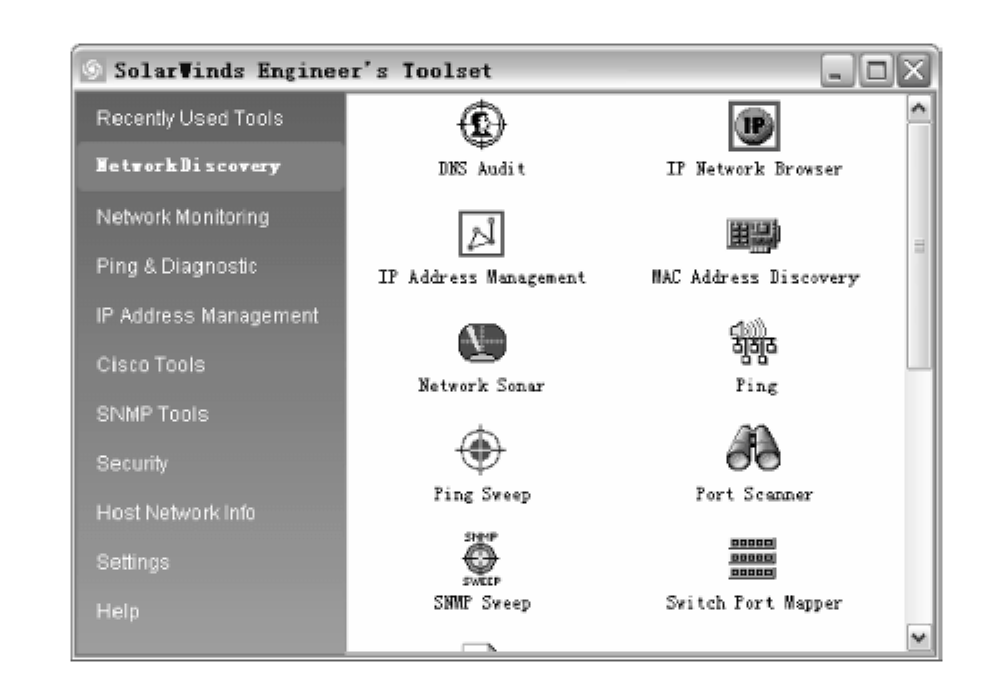


图 7-71　Network Discovery 窗口

(2) 在右侧栏中，双击 IP Network Browser 图标，显示图 7-72 所示的 IP Network Browser 窗口。在该窗口中，提供以下 3 种扫描方式。

① Scan a Single Device：该方式只扫描用户指定的单个网络设备。

② Scan a Subnet：使用该方式，可以扫描一个网络段内的所有设备。

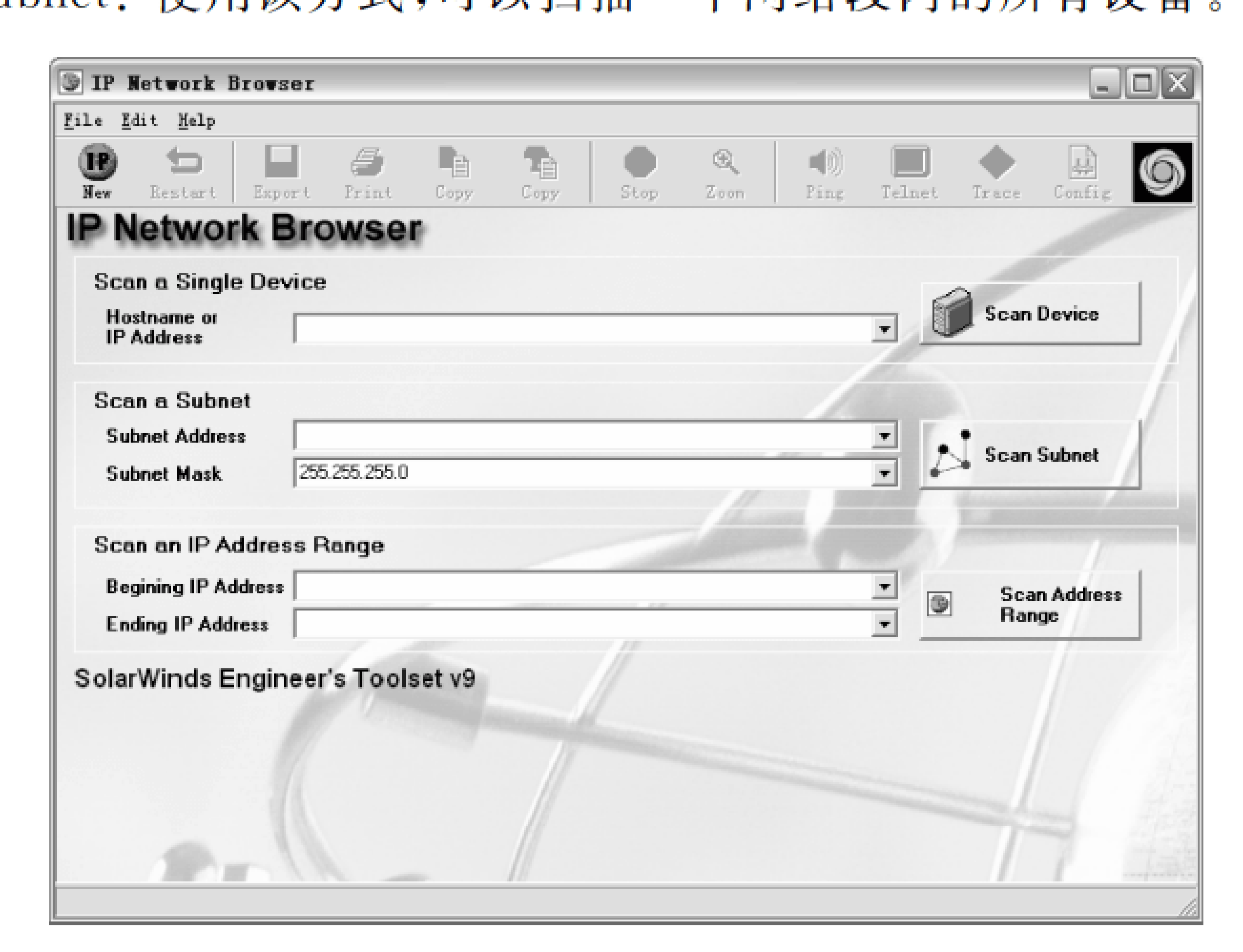


图 7-72　IP Network Browser 窗口

③ Scan an IP Address Range：使用该方式，可以扫描一个地址段内的所有设备。

这里使用 Scan an IP Address Range 方式，扫描一个地址段的设备。在 Beginning IP Address 和 Ending IP Address 文本框中，分别输入所要扫描的起始地址和结束地址。

（3）单击 Scan Address Range 按钮，即可开始扫描，扫描完成后，显示图 7-73 所示的对话框。

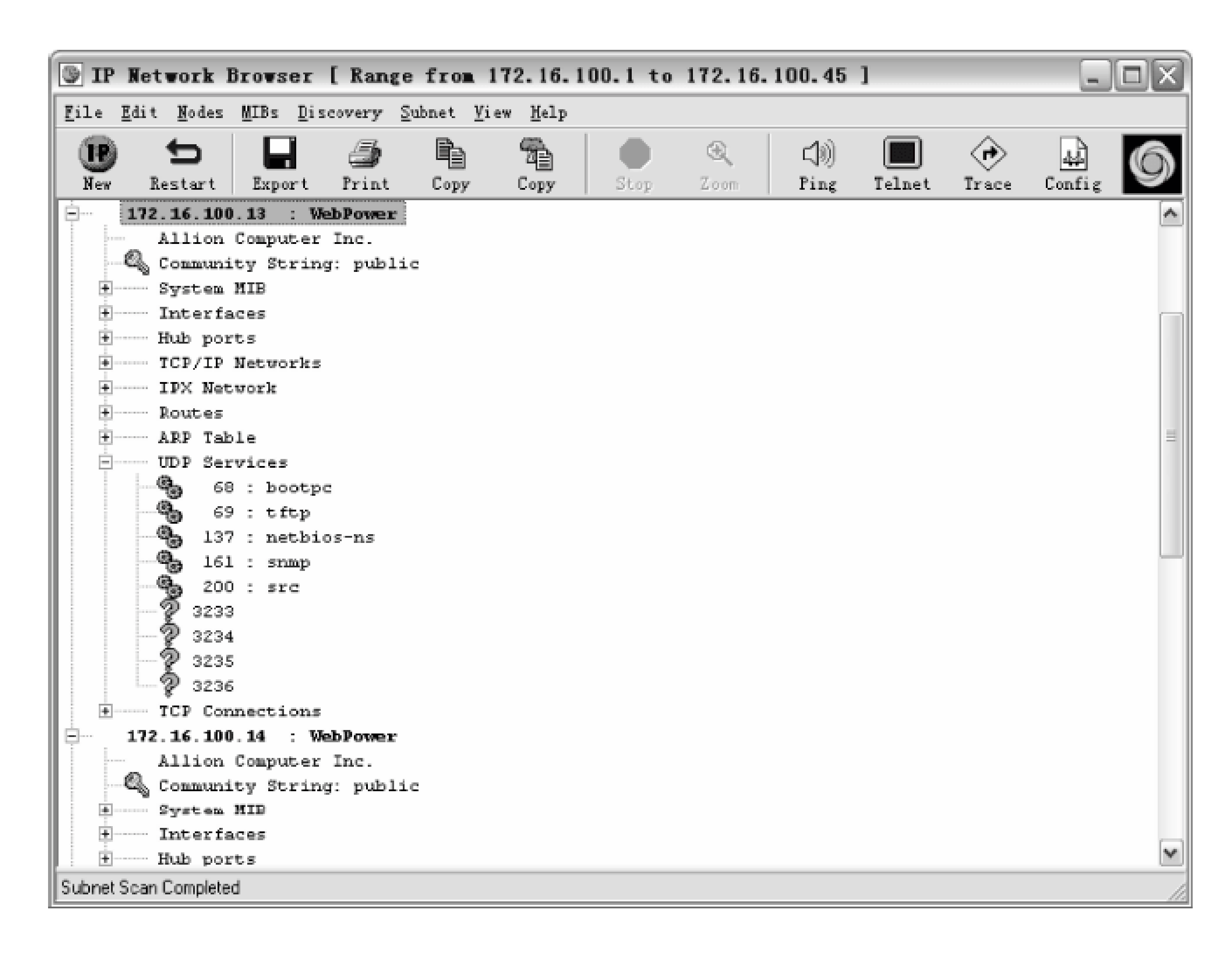


图 7-73　扫描结果

另外，还可以根据需要打印或导出扫描结果，在 IP Network Browser 窗口中，单击 print 按钮，直接打印扫描结果。也可以按如下步骤导出扫描结果：

（1）在 IP Network Browser 窗口中，单击 Export 按钮，显示图 7-74 所示的 Export Wizard 对话框。根据需要在 Which nodes would you like to include 列表中选中想要导出的设备信息。

（2）单击 Next 按钮，显示图 7-75 所示的导出内容对话框。在 Which discovery groups would you like to include 列表中，选中想要导出的信息，单击 Select All 按钮，可以选中所有信息。

（3）单击 Next 按钮，显示图 7-76 所示的对话框，提示是否导出 SNMP 字符串。用户可根据需要进行选择，这里选中 Yes 单选按钮，即导出 SNMP 字符串。

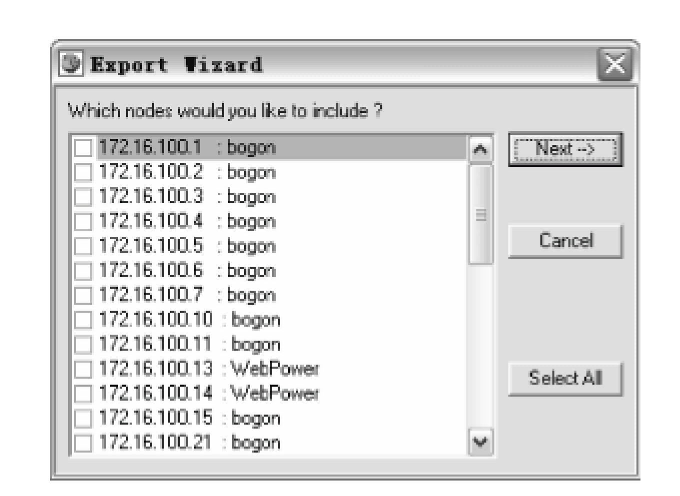


图 7-74　Export Wizard 对话框

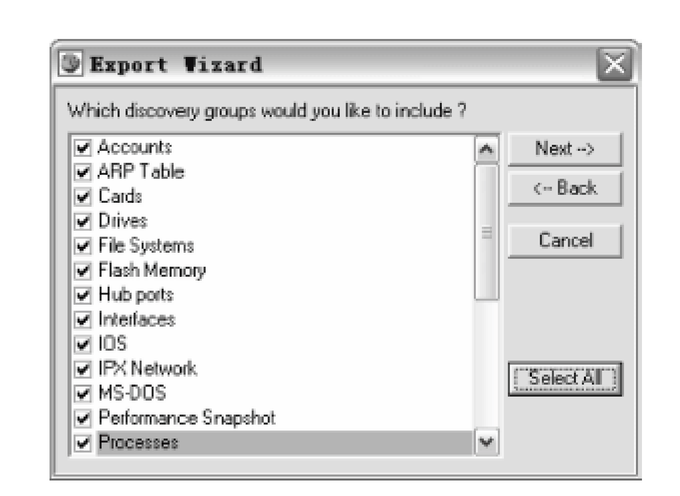


图 7-75　导出内容

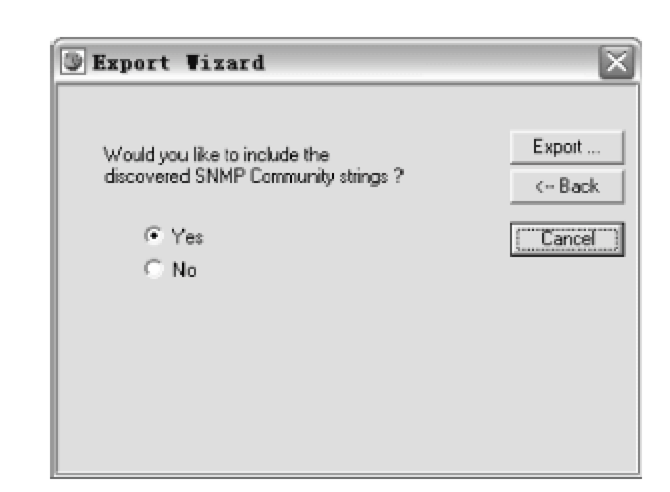


图 7-76　提示是否导出 SNMP 字符串

（4）单击 Export 按钮，打开 Export to 对话框，根据需要选择所要保存的目录即可。

（5）单击 Save 按钮，完成导出操作。

4. 查询 CPU 负载

Advanced CPU Load 可以监视路由器、交换机和服务器的 CPU 使用率，并可查看实时和历史使用率。

（1）在软件主窗口左侧栏中，选择 NetworkMonitoring 选项，显示图 7-77 所示的 NetworkMonitoring 窗口。

（2）在右侧栏中，双击 Advanced CPU Load 图标，打开 Advanced CPU Load 窗口。依次选择 File→New Advanced CPU Load Database，显示图 7-78 所示的 New Advanced CPU Load Database 对话框。根据需要设置新建的数据库的保存位置，并在"文件名"文本框中，输入欲保存的名称。

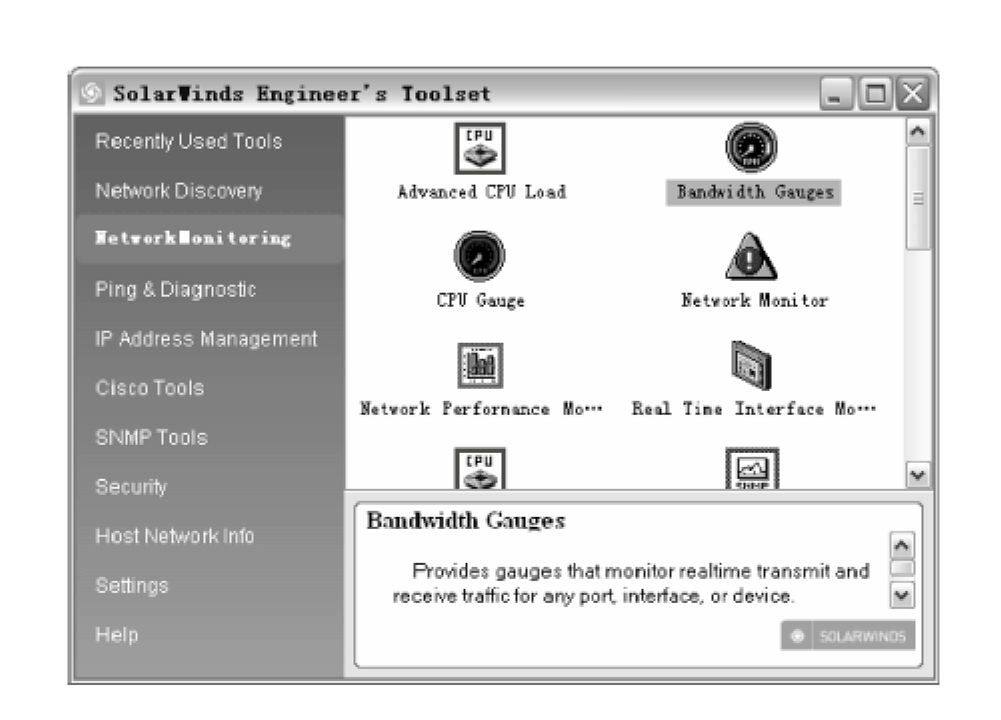


图 7-77　NetworkMonitoring 窗口

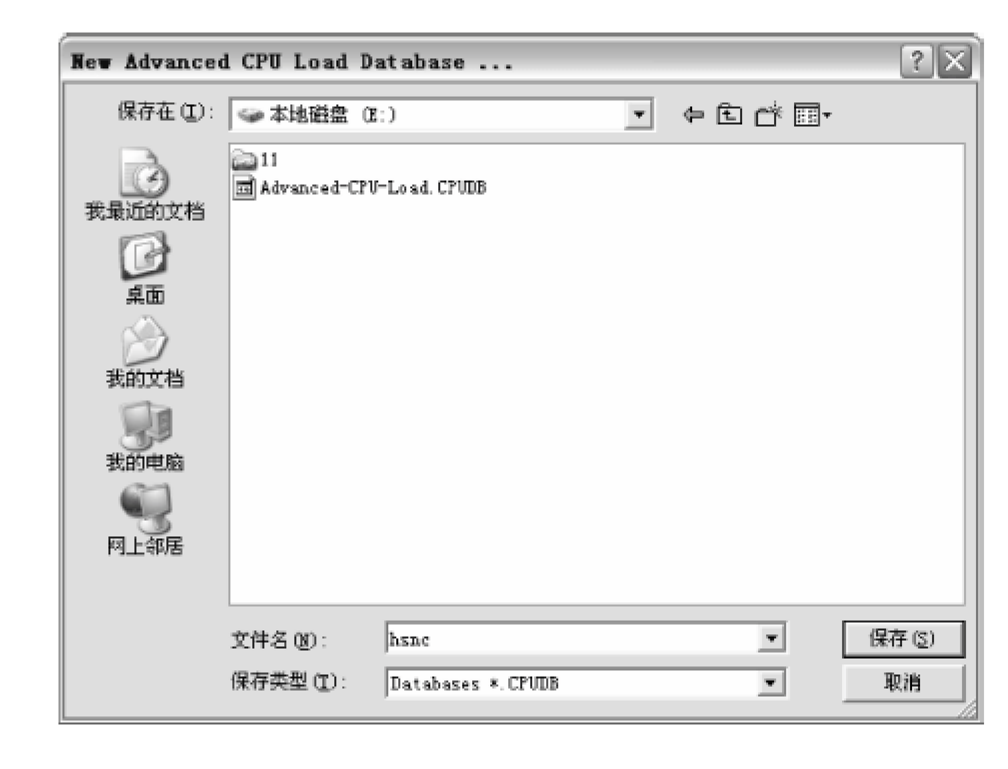


图 7-78　New Advanced CPU Load Database 对话框

（3）单击"保存"按钮，返回 Advanced CPU Load 窗口，如图 7-79 所示。

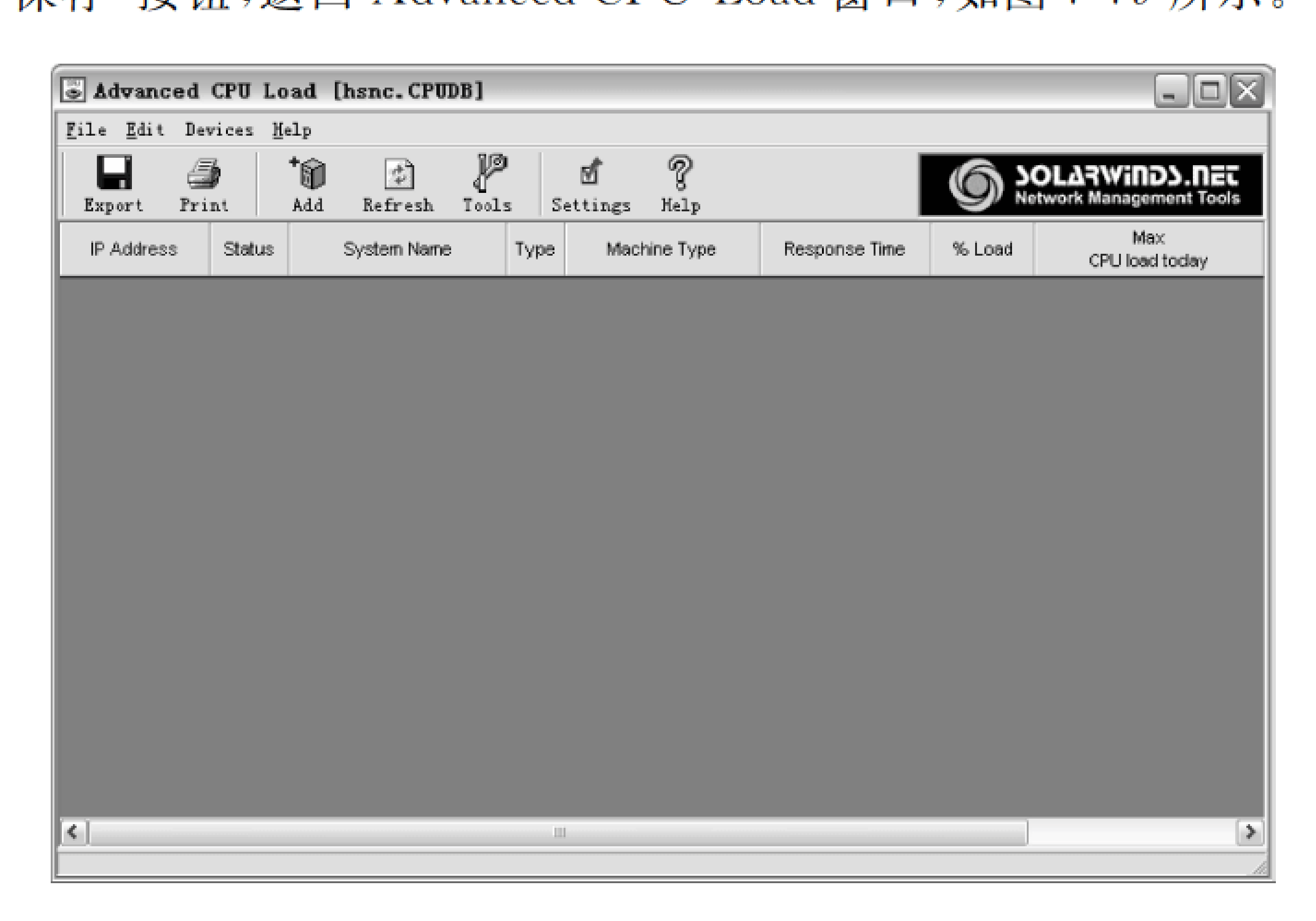


图 7-79　新建的查询

（4）单击 Add 按钮，显示图 7-80 所示的 Add Network Device 对话框。分别在 IP Address or Hostname 和 SNMP Community String 文本框中，输入欲添加设备的 IP 地址和

SNMP 字符串。

（5）单击 OK 按钮，添加设备成功，该设备即可显示在 Advanced CPU Load 窗口中，如图 7-81 所示。重复操作，可添加多台设备。

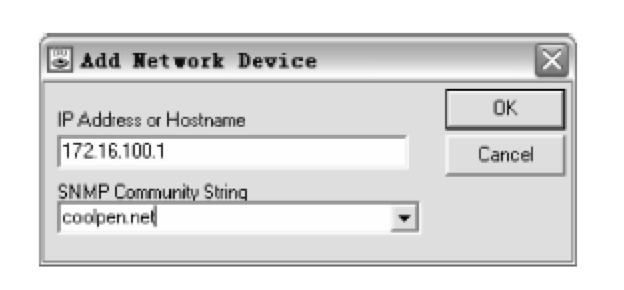


图 7-80　Add Network Device 对话框

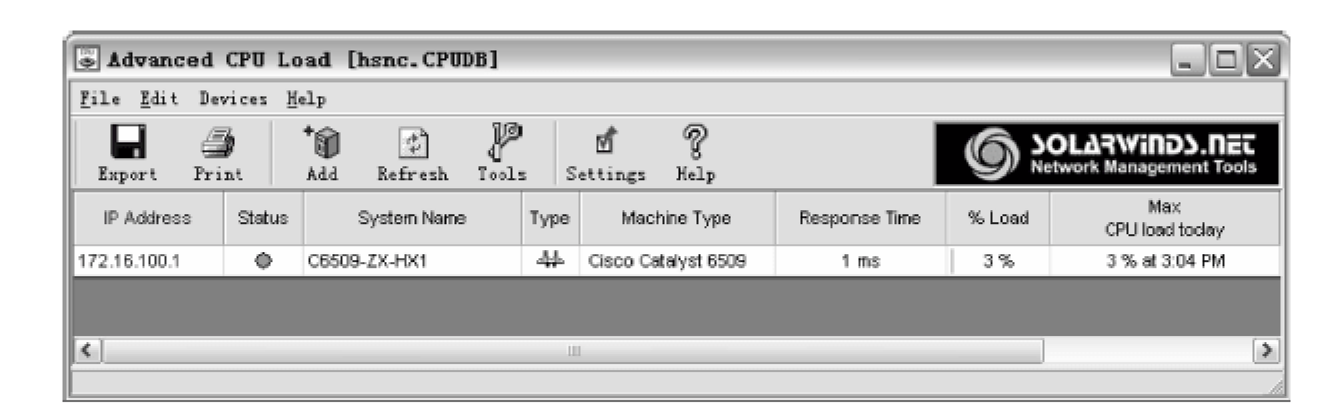


图 7-81　成功添加设备

（6）右击想要查看详细信息的设备，在快捷菜单中选择 Edit Device Details 命令，显示图 7-82 所示的 C4006-ZX-HJ details 窗口。在该窗口中，可以查看描述信息、设备类型、响应延时、当前 CPU 负载情况、处理器数量、最后启动时间、最后发生错误的时间、下一次测试时间和 OID 信息。另外，还可以对设备进行简单配置，例如系统名称、IP 地址、SNMP 字符串等。

（7）如果修改了设备的配置，需要单击 Apply Changes 按钮，保存修改。

（8）右击想要查看的详细信息的设备，在快捷菜单中选择 Historical Graph 命令。显示图 7-83 所示的 CPU Load on C4006-ZX-HJ 对话框。在该对话框中，可以查看设备当前的 CPU 使用率，以及最近一个月的 CPU 使用情况。

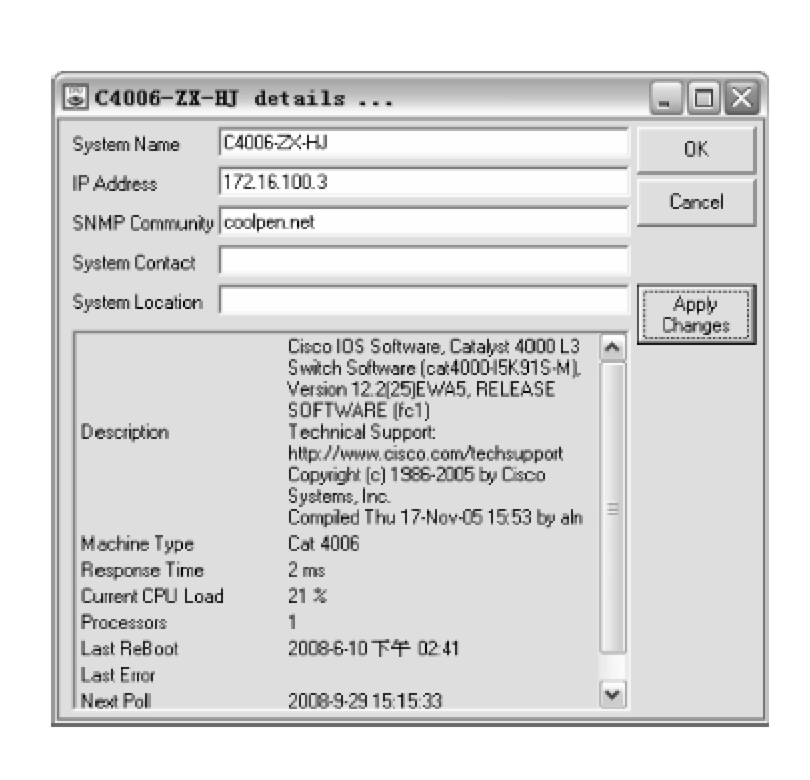


图 7-82　C4006-ZX-HJ details 窗口

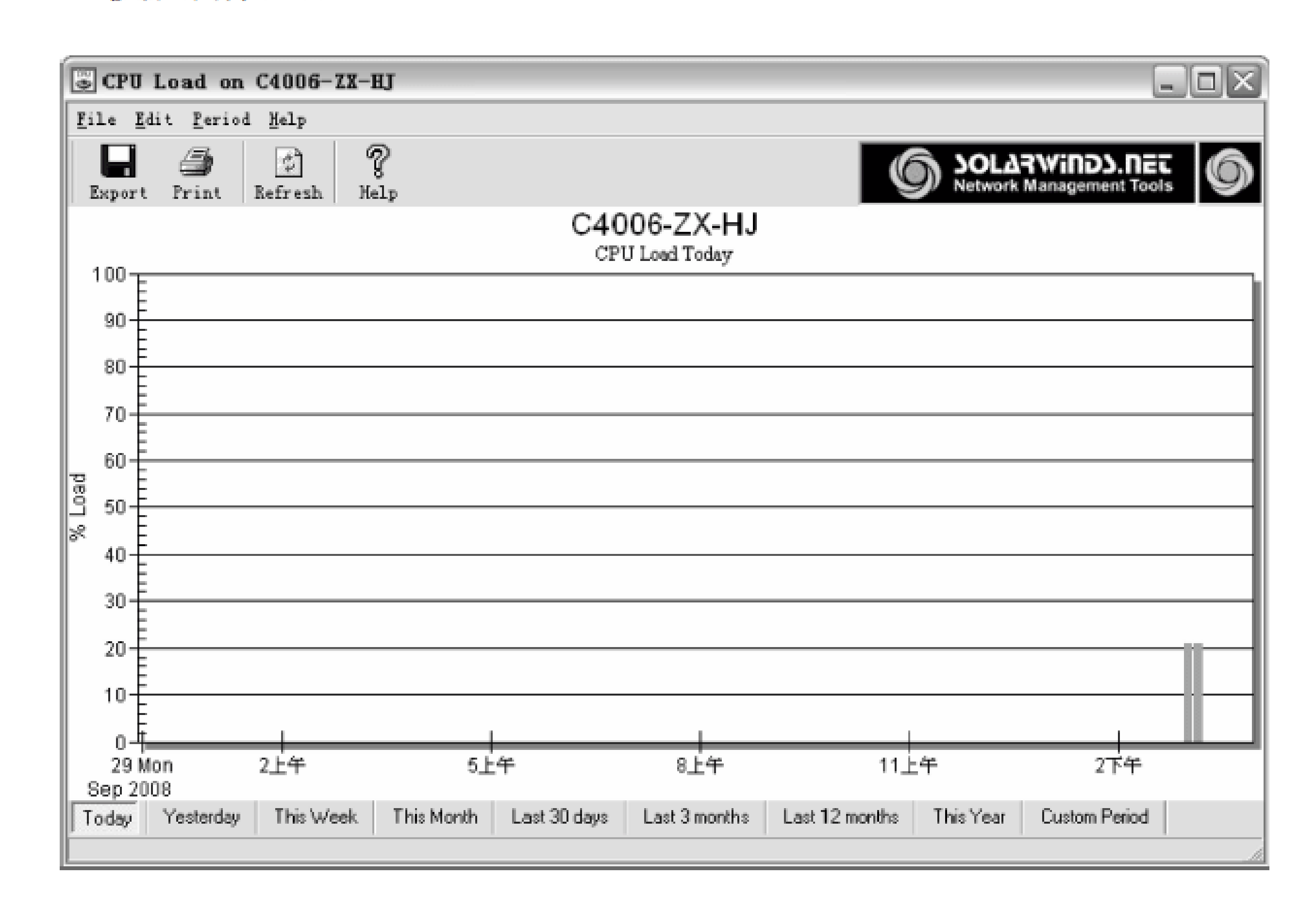


图 7-83　查看 CPU 历史负载情况

5. 带宽测试

Bandwidth Gauges 提供实时监控任何端口的传输和接收，以及接口或设备通信。

（1）在 NetworkMonitoring 窗口中，在右侧栏中双击 Bandwidth Gauges 图标，显示图 7-84 所示的 Bandwidth Gauges 对话框。

（2）依次选择 Gauges→New Gauges 命令，显示图 7-85 所示的 Device and Credentials 对话框。在 Device or IP address 和 Community string 下拉列表框中，分别输入欲监控的设备的 IP 地址和 SNMP 字符串。

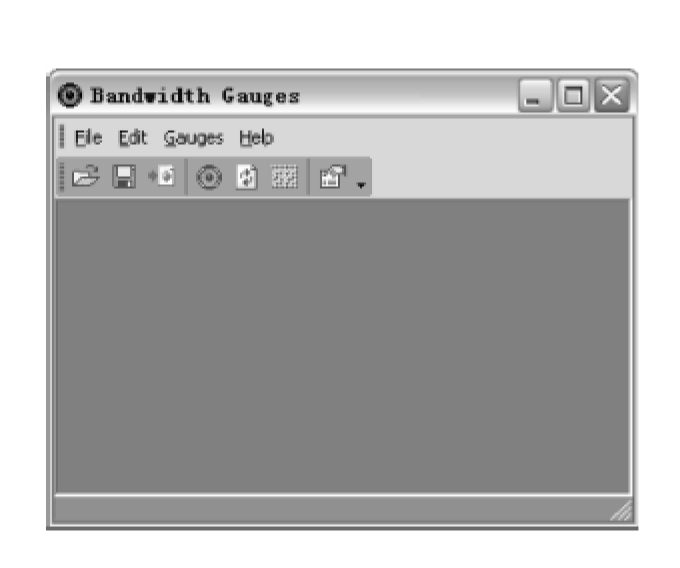


图 7-84　Bandwidth Gauges 对话框

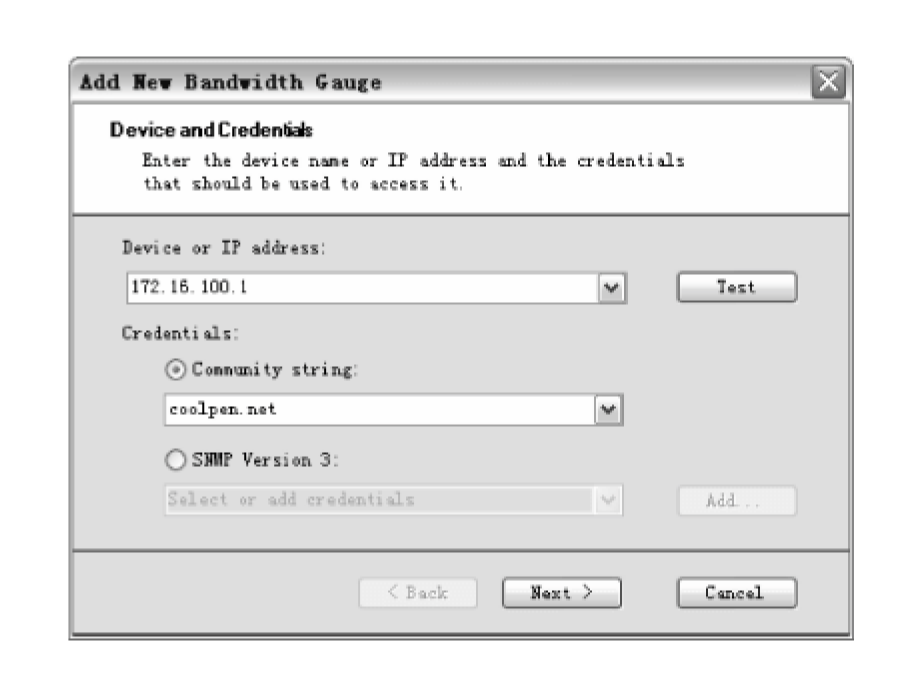


图 7-85　Device and Credentials 对话框

（3）单击 Test 按钮，测试是否可以监控目标设备，测试完成后，显示图 7-86 所示的 Credentials Test 对话框。从图中可知，目标设备已经通过测试。

（4）单击 OK 按钮返回，再单击 Next 按钮，显示图 7-87 所示的 Interface/Port 对话框。在 Interface/Port 列表中，选择欲监控的端口。

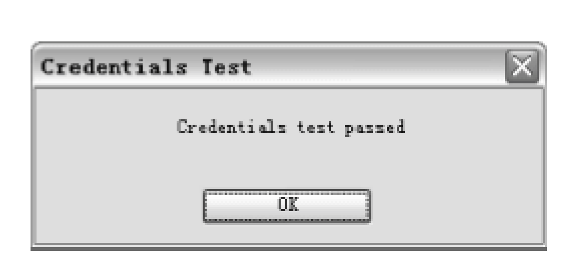


图 7-86　通过测试

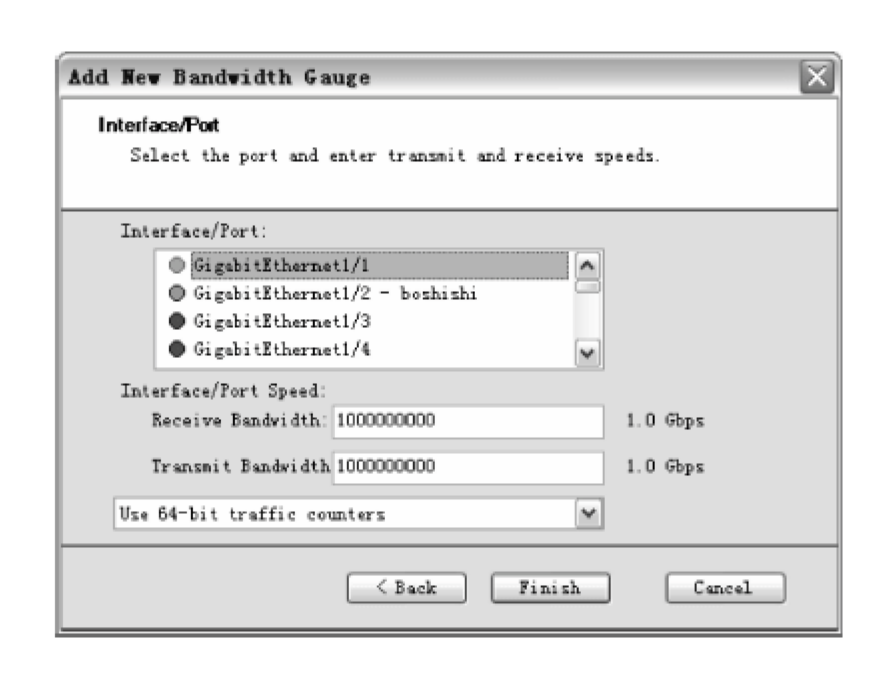


图 7-87　Interface/Port 对话框

（5）单击 Finish 按钮，即可开始监控目标端口的带宽，如图 7-88 所示。其中，Receive 表示接收速率，Transmit 表示传输速率。

6．CPU Gauge 的使用

CPU Gauge 提供实时 Cisco 设备的 CPU 负载情况，并以图形形式进行显示。

（1）在 NetworkMonitoring 窗口中，双击 CPU Gauge 图标，显示 CPU Gauge 窗口。单击窗口右上角的按钮，如图 7-89 所示。

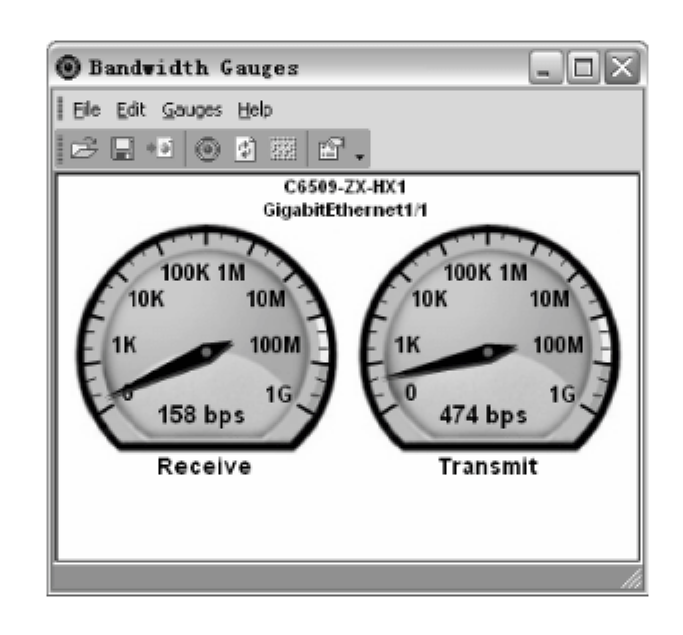


图 7-88　端口带宽测试

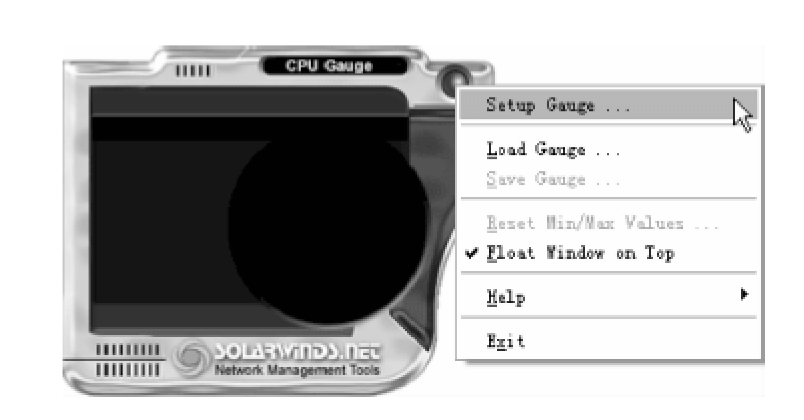


图 7-89　CPU Gauge 功能菜单

(2) 在快捷菜单中，选择 Setup Gauge 命令，显示图 7-90 所示的 Setup CPU Gauge 对话框。在 IP Address or Hostname 和 SNMP Community String 文本框中，分别输入所要查看设备的 IP 地址和 SNMP 字符串。

(3) 单击 OK 按钮，即可显示图 7-91 所示的设备的 CPU 的使用情况。在对话框的上方，显示该设备的名称，这里设置设备名称为 C4506-ZX-HX1。

单击 按钮，并选择 Save Gauge 命令，可以将当前设备 CPU Gauge 进行保存，如图 7-92 所示。

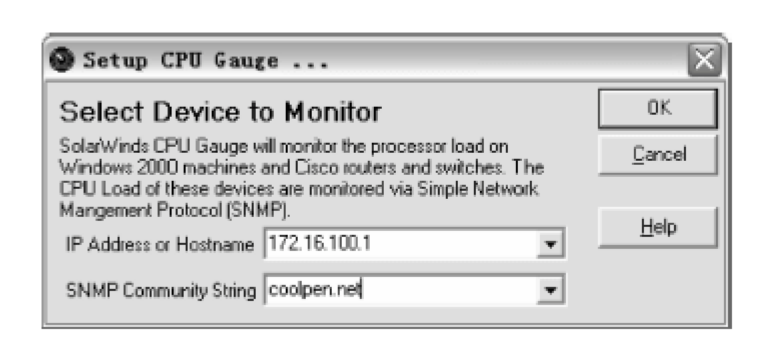


图 7-90 Setup CPU Gauge 对话框



图 7-91 目标设备的 CPU 使用情况

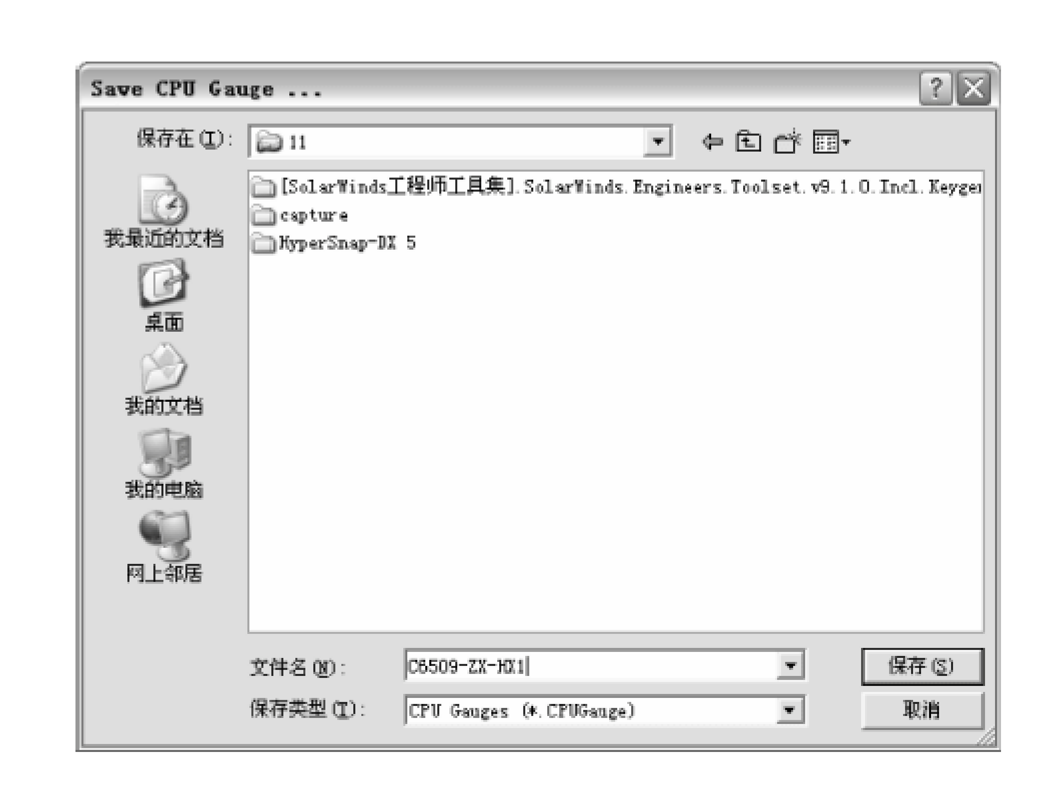


图 7-92 保存 CPU Gauge

7. 网络性能监视器

Network Performance Monitor 提供实时网络监控、跟踪网络延迟数据包丢失、Traffic、带宽使用等网络统计信息。

(1) 在 NetworkMonitoring 窗口中，双击 Network Performance Monitor 图标，显示图 7-93 所示的 Network Performance Monitor 窗口。

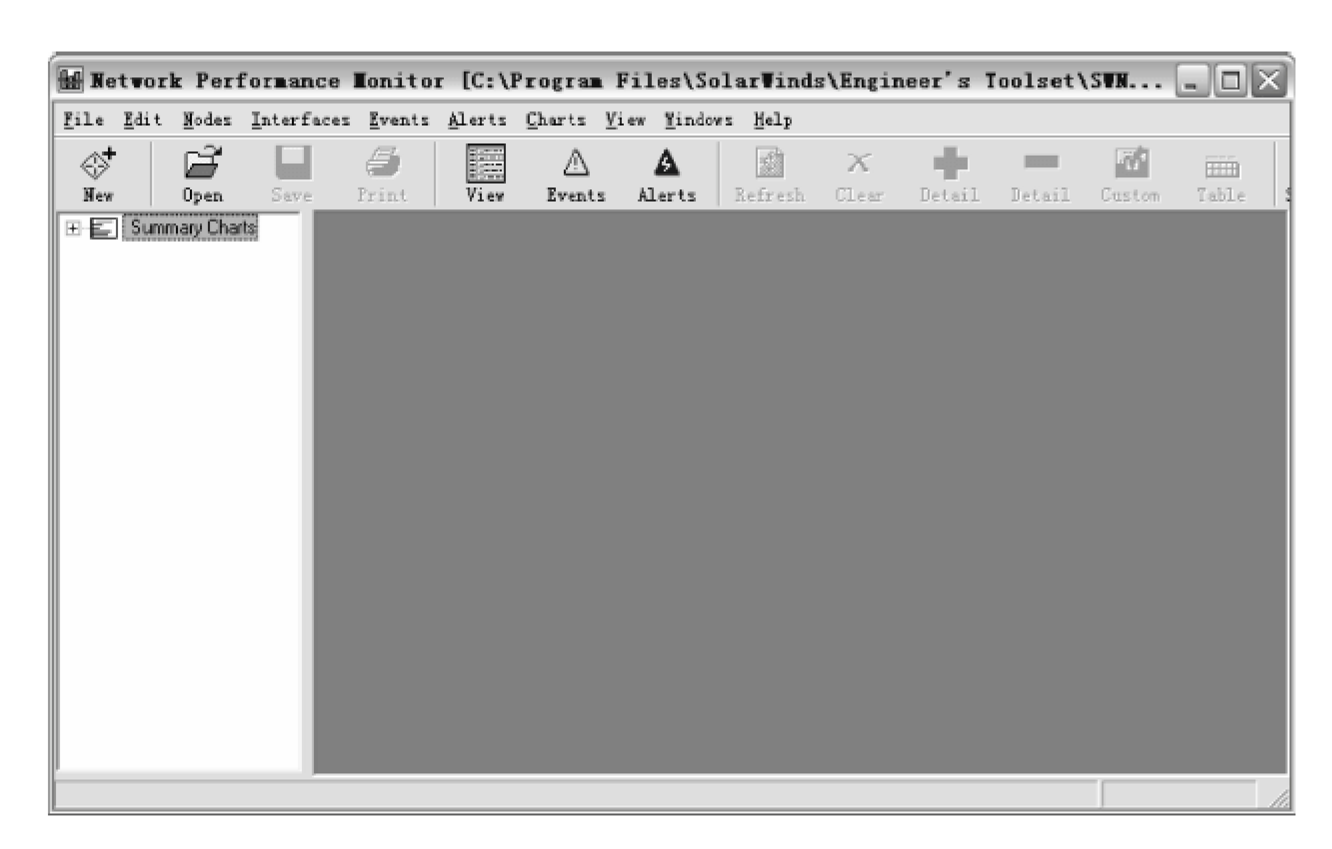


图 7-93 Network Performance Monitor 窗口

(2) 单击 New 按钮，显示图 7-94 所示的 Device 对话框。在 Device or IP address 下拉列表框中，输入需要进行性能监视的主机、服务器、路由器等网络设备地址。

（3）单击 Next 按钮，显示图 7-95 所示的 Credentials 对话框。在 Credentials 选项区域中，选择所使用 SNMP 的版本号，这里选中 Community string 单选按钮，并在下拉列表框中输入其 SNMP 字符串。需要注意的是，如果选中 Device does not support SNMP 单选按钮，则可以监视不支持 SNMP 协议的设备，但只能监视其响应时间和丢包率。

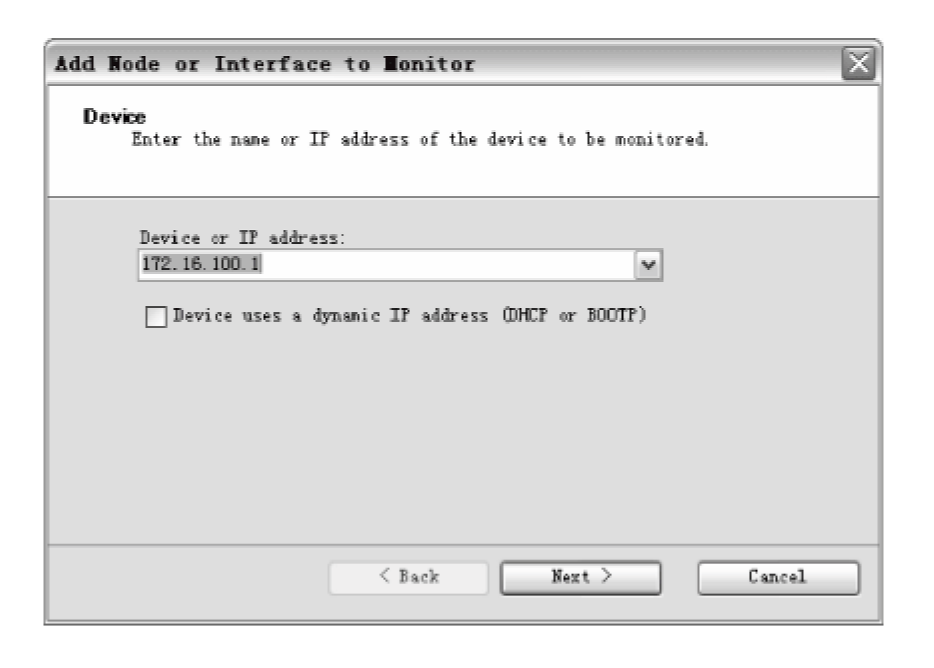


图 7-94 Device 对话框

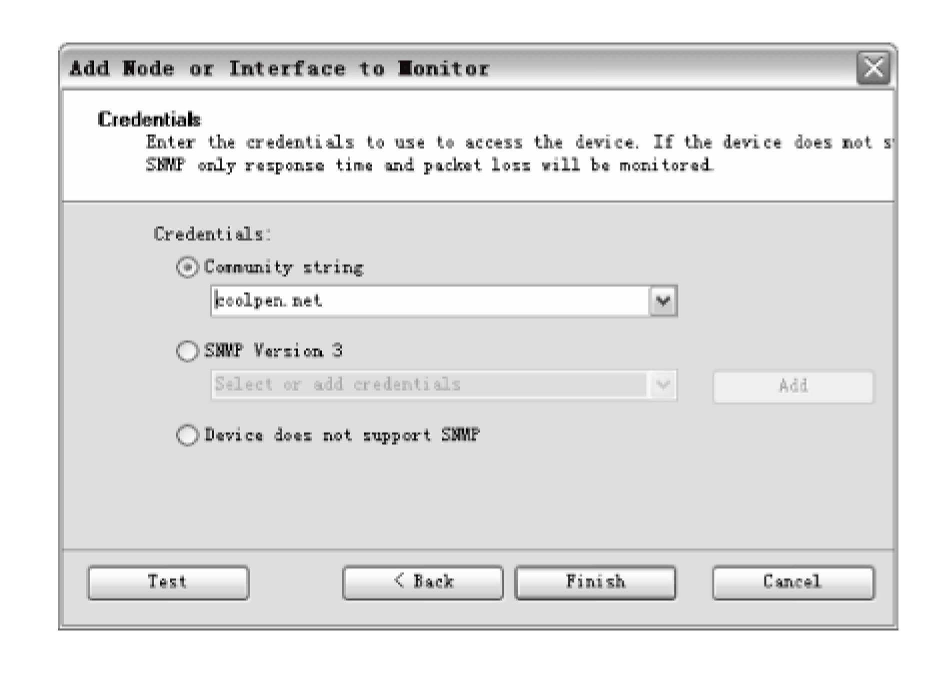


图 7-95 Credentials 对话框

（4）单击 Finish 按钮，显示图 7-96 所示的 Resources on C4506-ZX-HX1 窗口。根据需要选择所要监视的端口，如果单击 Select All 按钮，则可以监视全部端口，如果单击 Select All Active Interfaces 按钮，则可以监视当前处于活动状态的端口。

（5）单击 OK 按钮，返回 Network Performance Monitor 窗口，在左侧栏中展开新添加的设备，即可查看监视该设备的各个端口及 VLAN 信息，如图 7-97 所示。其中，在左侧栏中，各选项的含义如表 7-1 所示。

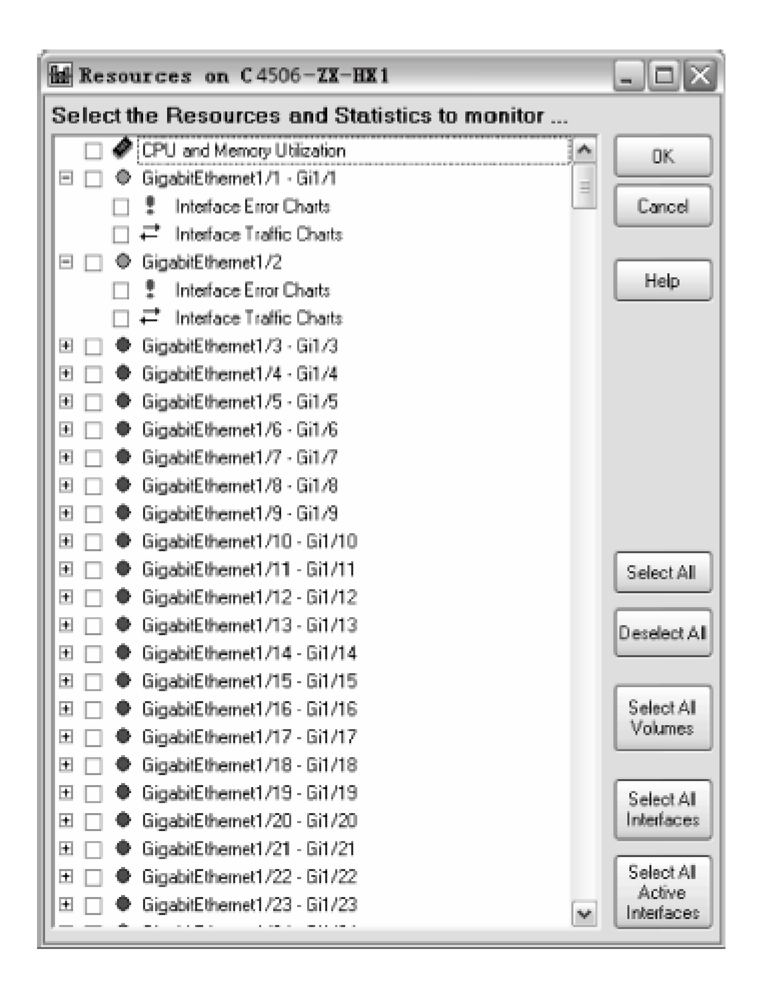


图 7-96 Resources on C4506-ZX-HX1 窗口

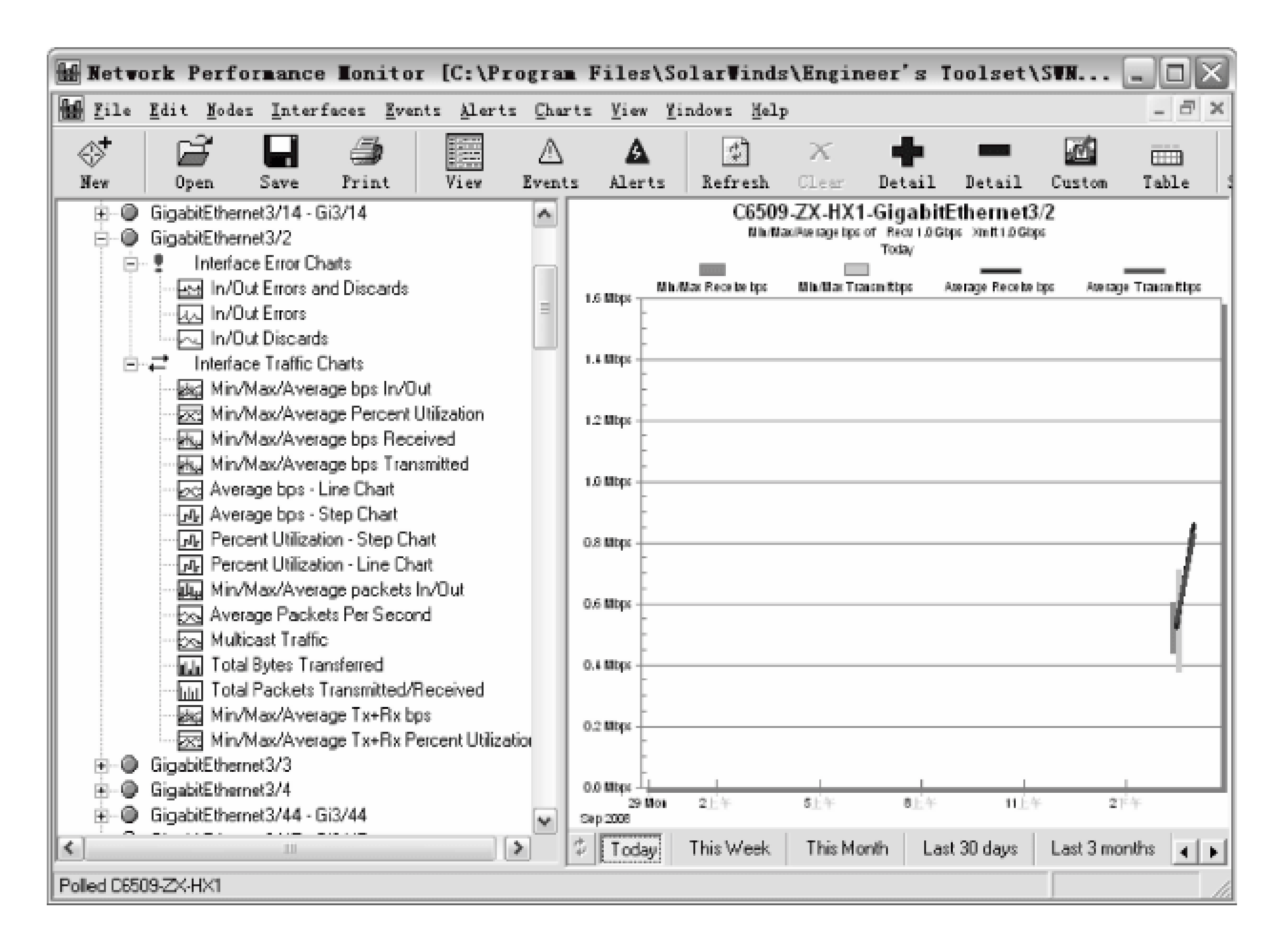


图 7-97 监视端口

（6）右击某接口，在快捷菜单中选择 Interface Details 命令，可以显示接口详细信息，如图 7-98 所示。包括 MIB-2 中 Interface 对象组中所有对象、数据传输速率，接口利用率，丢包率，错误率等详细的信息。如果单击 Administratively Shutdown Interface 按钮，可以关闭该接口。

表 7-1 网络性能监视器各选项含义

表 项 名 称	含　　义
Min/Max/Average bps In/Out	最小/最大/平均数据传输速率，接收与传输使用不同颜色分别列出。每 5 分钟取一次值，(可以通过设置修改取值间隔)色柱上下两端分别表示最大值与最小值，不同颜色线表示平均值的连线(同样是 5 分钟取一次值)
Min/Max/Average Percent Utilization	最小/最大/平均利用率，图表显示与第一项类似
Min/Max/Average bps Received	接收的最小/最大/平均数据传输速率，为第一项的表的接收部分
Min/Max/Average bps Transmitted	传输的最小/最大/平均数据传输速率
Average bps - Line Chart	用线形图分别表示接收和传输速率
Average bps - Step Chart	用柱形图分别表示接收和传输速率
Min/Max/Average packets In/Out	最小/最大/平均数据包传输速率
Average packets Per Second	以线形图方式显示，为 Min/Max/Average packets In/Out 的一部分
Multicast Traffic	分别显示接收、传输广播数据传输速率
Total Bytes Transferred	用柱形图分别表示当天接收与传输的总字节数
Total Packets Transmitted/Received	用柱形图分别表示当天接收与传输的总数据包数

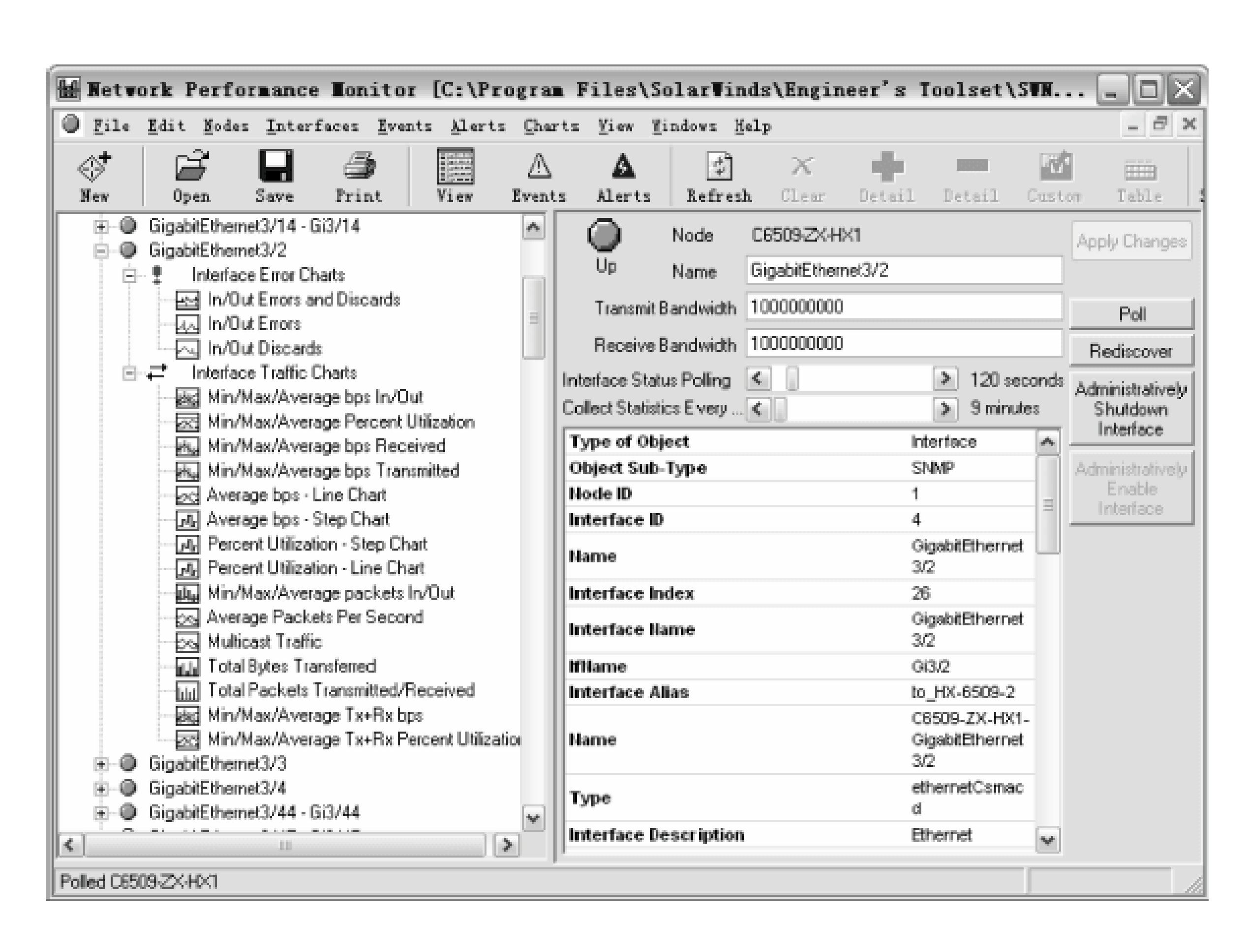


图 7-98　端口详细信息

(7) 单击工具栏中的 View 按钮，可以分组显示性能参数，如图 7-99 所示。其中，部分选项的含义如表 7-2 所示。

表 7-2 分组显示部分内容含义

分 组 类 型	说　　明
Nodes View	显示所监视的所有节点信息
Response Time	显示所有节点的响应时间
Last Time each Node Rebooted	各节点最后一次重新启动时间
Interface Status	各节点的各接口状态
Interface	显示各节点所被监视的接口名称等
Last Time Each Interface Changed	各节点接口状态最后一次改变的时间
Current Traffic	当前各接口接收和传输速率、利用率

续表

分 组 类 型	说　　明
Interface Bandwidth Settings	各接口带宽显示
Maximum Traffic Load Today	当天各接口的最大负载
Current Packs per Second	当前各接口的数据包接收传输速率
Current Packs Size	当前接收传输数据包大小
Errors and Discards - This Hours	当前一小时错误和丢包数
Errors and Discards - Today	当天错误和丢包数
Node Polling Intervals	节点轮询时间间隔
Interface Polling Intervals	各节点轮询时间间隔
Percent Utilization	当前各接口接收传输利用率
IOS Image Version	Cisco 设备系统镜像文件版本信息

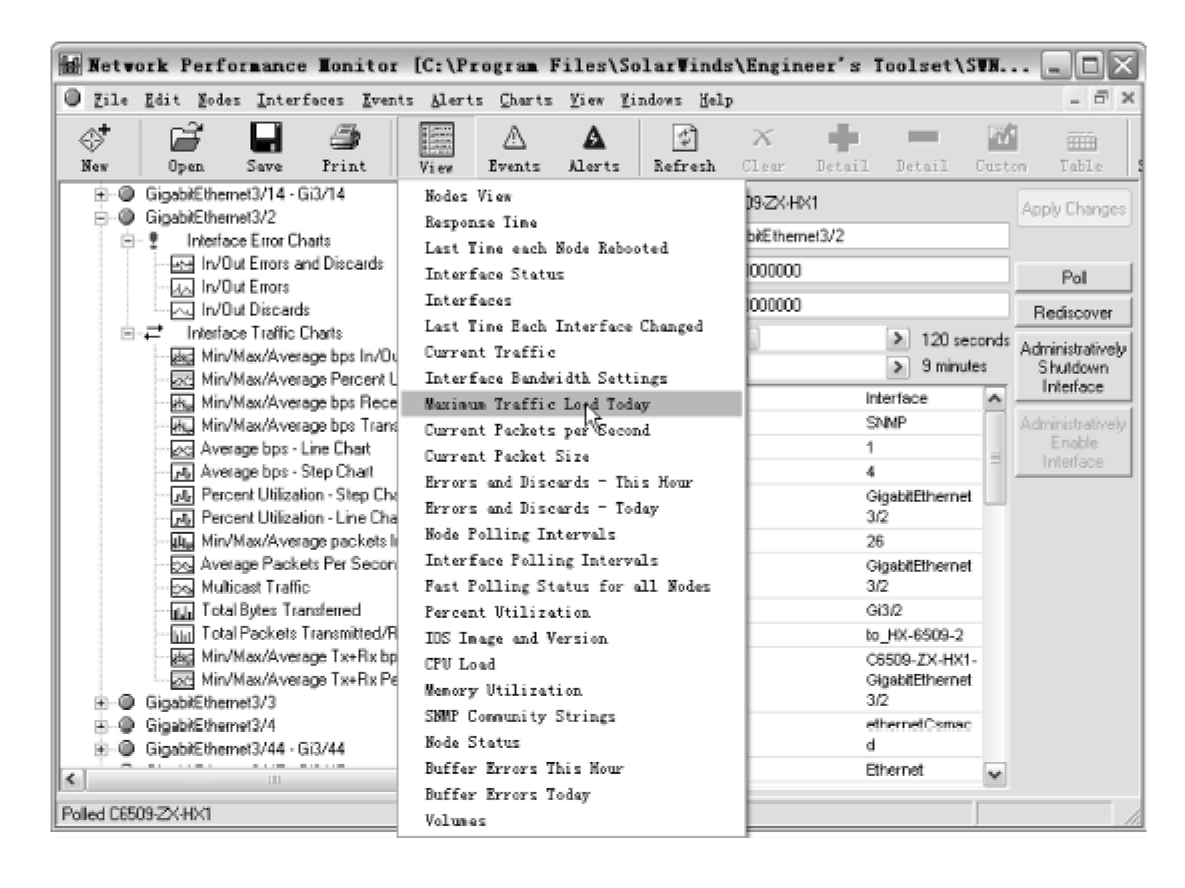


图 7-99　分组显示性能参数

习题

1. 简述 MRTG 的特点。
2. SolarWinds Engineer's Toolset 提供哪些监视信息？

实验：SolarWinds 分析网络吞吐量

实验目的：

掌握 SolarWinds 的使用方法。

实验内容：

使用 SolarWinds 监视网络设备。

实验步骤：

（1）安装 SolarWinds。

（2）发现网络。

（3）查询网络设备 CPU 负载。

（4）测试网络带宽。

（5）使用网络性能监视器。

第 8 章 chapter 8

网络链路管理

网络链路的正常连接，是计算机正常接入网络的基础，例如，交换机、路由器等网络设备的连接与配置不正确，网卡和网络协议配置错误，计算机的 IP 地址信息设置不正确等都会造成 IP 链路的连接问题。只有 IP 链路畅通，计算机设备才能够正常接入网络。因此，需要使用一些测试软件来判断网络逻辑链路是否畅通。

8.1 网络链路管理规划

网络链路是网络的基础部分，对于有线网络只有使用双绞线或光纤正常连接才能保证网络的畅通，因此网络链路的管理也是管理员日常工作的重点。

8.1.1 项目背景

在当前网络中，除客户端计算机连接交换机使用 100Mbps 双绞线外，其他连接均采用 1000Mbps 连接。其中，服务器与其连接的交换机所使用的是 1000Mbps 双绞线，其他 1000Mbps 连接均采用光纤连接。

8.1.2 项目需求

虽然网络链路发生故障的可能性比较低，但并不是完全不会发生故障。在网络链路发生故障时，需要及时使用相关工具进行故障排查。通常情况下，网络链路故障分为网络物理链路故障和逻辑链路故障。

8.1.3 解决方案

对于网络链路故障通常可以通过如下 3 种方法解决。

(1) 对于双绞线链路测试，管理员可以使用 Fluke MircoScanner^2 来进行测试，而在各科室中可以配备价格比较便宜的双绞线测线仪，在该项目中配备“能手”测线仪。

(2) 对于光纤链路除可通过网络设备上的指示灯查看外，还可通过 Fluke DTX 系列电缆认证分析仪进行测试。

(3) 对于逻辑链路连接问题，可以通过 Windows 自带的测试工具进行连通性连接，例如 IP 网络连通性测试工具(Ping)、路径信息提示工具(Pathping)和测试网络路由路径(Tracert)。

8.2　网络物理链路测试

物理链路是计算机连接网络的基础，连通性故障在网络初创阶段、网络拓扑调整之后，以及网络运行 3～5 年后可能会大量发生。通常情况下，对于网络连接故障往往只需简单地做一下网络布线的连通性测试，即可定位故障原因、找到故障点，从而迅速隔离和排除故障。

8.2.1　Fluke MircoScanner2

1. 简介

Fluke MicroScanner2 电缆检测仪是一款手持式测试仪器，如图 8-1 所示，用于检验和诊断双绞线和同轴电缆的接线，以及检测网络服务。它可执行下列工作。



图 8-1　Fluke MicroScanner2

(1) 最长可测量 1500ft(457m)的电缆，并检测双绞线和同轴电缆布线中的开路和短路问题。

(2) 检测双绞线布线中的线对串绕问题。

(3) 在一个屏幕上显示线序、电缆长度与开路位置的比例距离，以及远程 ID 号。

(4) 检测双绞线布线中的以太网端口并报告端口速度。

(5) 检测双绞线布线中的 PoE(以太网供电模块)和电话电压。

(6) IntelliTone 功能配合 Fluke Networks 的 IntelliTone 探头使用，可帮助查找和定位在墙壁中、接插板处或线束中的电缆。模拟音频发生器可与标准模拟探头配套使用，并包含能够可靠地识别线束中的电缆的 SmartTone 功能。

MicroScanner2 的组成及各种按钮如图 8-2 所示。

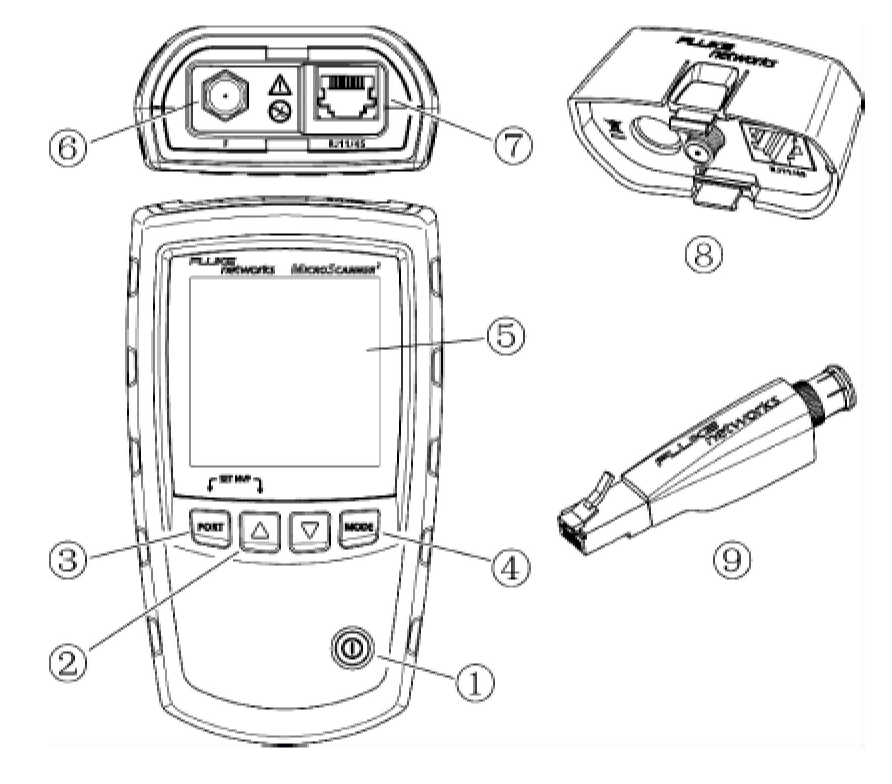


图 8-2　MicroScanner2 的按钮

(1) ON/OFF：开/关键。

(2) △/▽：导览屏幕和更改设置。在音频发生器模式下，用于在 IntelliTone 和模拟音频发生器的音调之间循环变换。

(3) PORT：选择 RJ-45 或同轴电缆连接器作为当前使用的端口。

(4) MODE：在电缆测试、音频发生器和 PoE 检测模式之间循环切换。

要进入其他模式，在启动测试仪的同时按住如下按键。

① PORT＋△：可用于校准长度测量值和选择米或英尺作为长度单位。

② MODE＋▽：激活演示模式，在该模式下测试仪显示测试结果屏幕的示例。

③ △＋▽：显示版本和序列号屏幕。

(5) 带背部照明的 LCD 显示屏。

(6) 用于连接到 75Ω 同轴电缆的 F-接头。

(7) 用于连接电话和双绞线网络电缆的模块式插孔。插孔可接插 8-针模块式(RJ-45)和 6-针模块式(RJ-11)接头。

(8) 带 F-接头和 8-针模块式插孔的线序适配器。

(9) 可选的带 F-接头和 8-针模块式插孔的远程 ID 定位器。

Fluke MicroScanner² 的显示屏组成信息如图 8-3 所示。

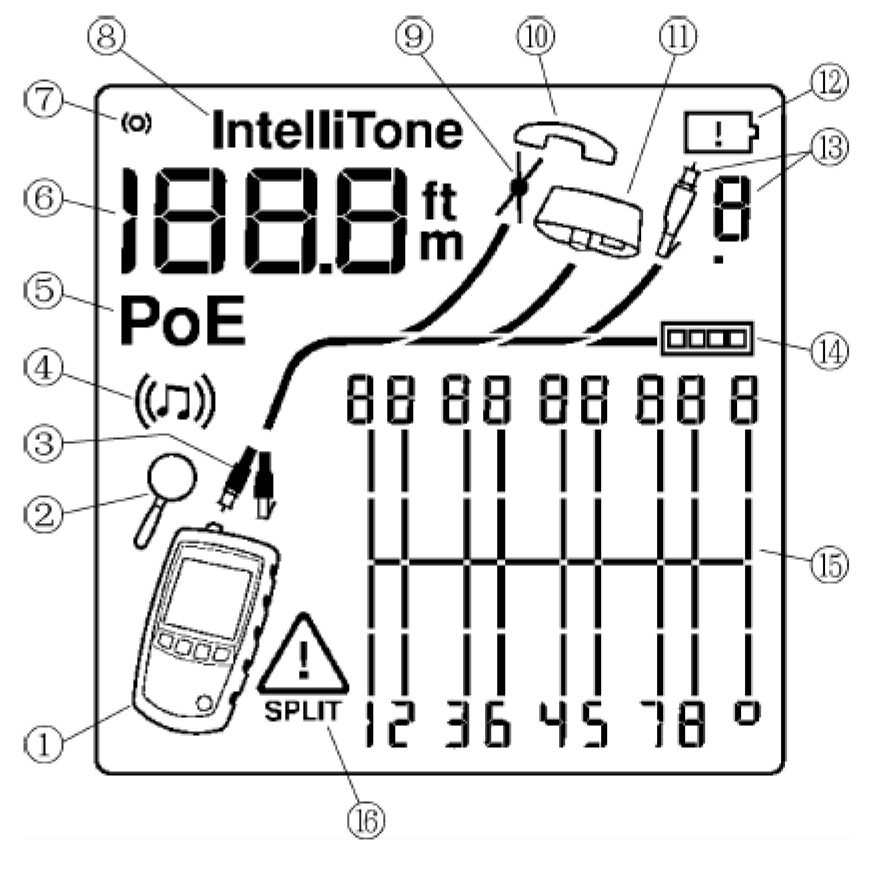


图 8-3 Fluke MicroScanner² 显示屏信息

(1) 测试仪图标。

(2) 细节屏幕指示符。

(3) 指示哪个端口为现用端口,RJ-45 端口还是同轴电缆端口。

(4) 音频模式指示符。

(5) 以太网供电模块指示符(PoE)。

(6) 带英尺/米指示符的数字显示。

(7) 测试活动指示符,在测试正在进行时会以动画方式显示。

(8) 当音频发生器处于 IntelliTone 模式时,会显示 IntelliTone。

(9) 表示电缆上存在短路。

(10) 电话电压指示符。

(11) 表示线序适配器连接到电缆的远端。

(12) 电池电量不足指示符。

(13) 表示 ID 定位器连接到电缆的远端并显示定位器的编号。

(14) 以太网端口指示符。

(15) 线序示意图。对于开路,线对点亮段的数量表示与故障位置的大致距离。最右侧的段表示屏蔽。

(16) "!"图标表示电缆存在故障或带有高压。当出现线对串绕问题时,显示 SPLIT(串绕)图标。

2. 跳线连通性测试

将需测试双绞线的一端插入 MicroScanner² 上的 RJ-11/45 端口,另一端插入线序适配器(如图 8-4 所示)端口。按 ON/OFF 按钮,打开电源开关。按动 MODE 按钮,直至在液晶显示屏上显示测试活动指示符。此时,将显示测试结果。测试结果均以数字表示,上面一行数字显示的是线序适配器一端插头处检测到的线路,下面一行显示的则是主机一端的实际接线情况。

(1) 链路连接正确

图 8-5 所示为连接正常完全没有故障的实例,并显示链路长度为 55.5m。

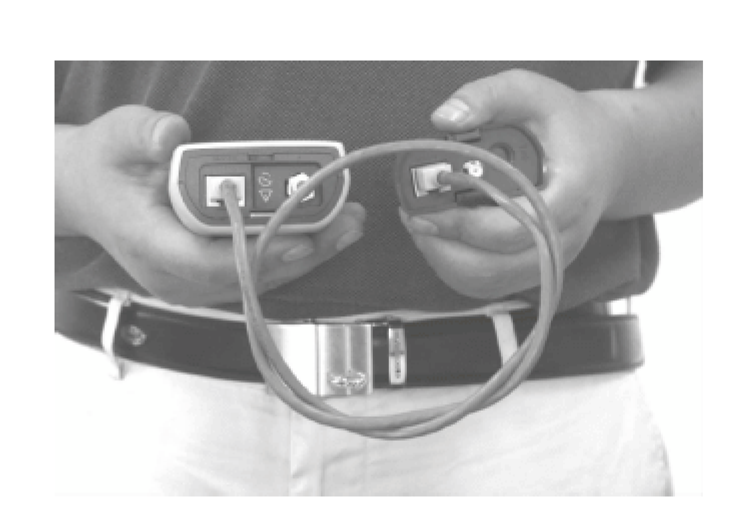


图 8-4 网线测试设备的连接

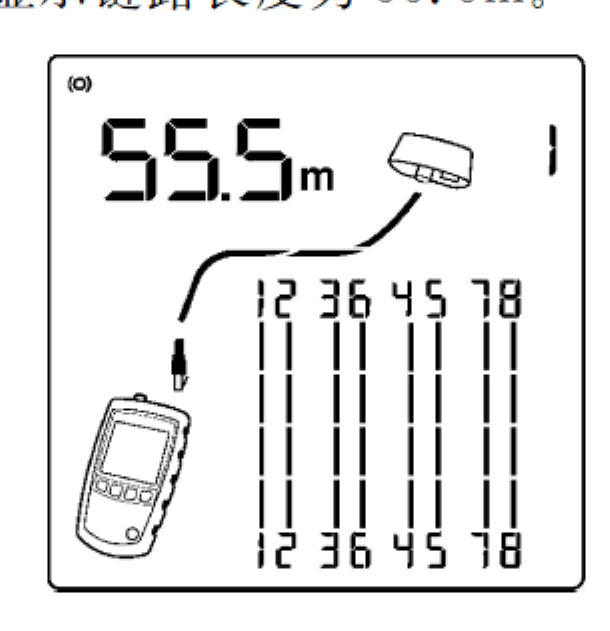


图 8-5 正常连通显示

(2) 链路存在开路

图 8-6 所示为第 4 根线上存在开路。电缆长度为 75.4m。开路中 3 个表示线对长度的线段表示开路大致位于线序适配器端距离的 3/4 处。若欲查看至开路处的距离，可以使用△/▽查看线对的单独结果。

注意：如果线对中只有一根线开路并且未连接线序适配器或远程 ID 定位器，线对中的两根线均显示为开路。如果线对中的两根线均开路，警告图标不显示，因为线对开路对某些布线应用属于正常现象。

(3) 链路存在短路

图 8-7 所示为第 5 根和第 6 根线之间存在短路，短路的接线会闪烁来表示故障。电缆长度为 75.4m。

注意：当存在短路时，远端适配器和未短路接线的线序不显示。

(4) 线路跨接

图 8-8 所示为第 3 根和第 4 根线跨接，线位号会闪烁来表示故障。电缆长度为 53.9m。电缆为屏蔽双绞线。

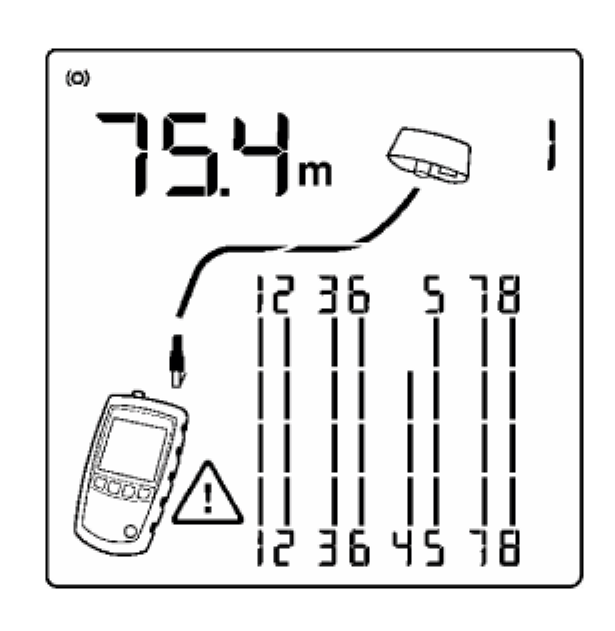


图 8-6　链路存在开路

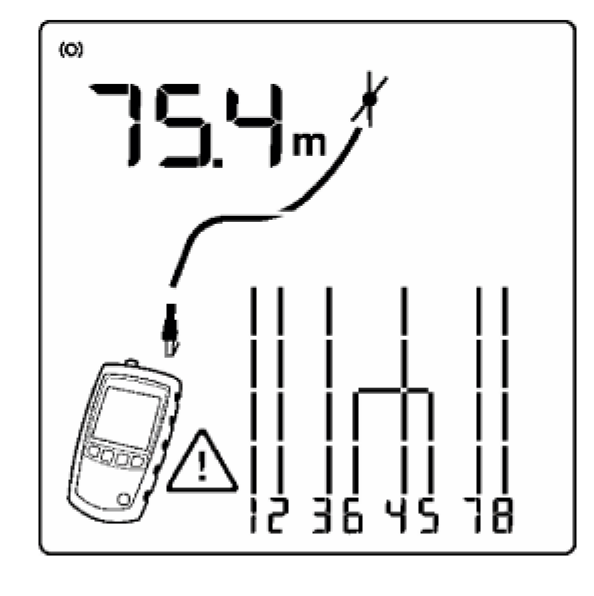


图 8-7　链路存在短路

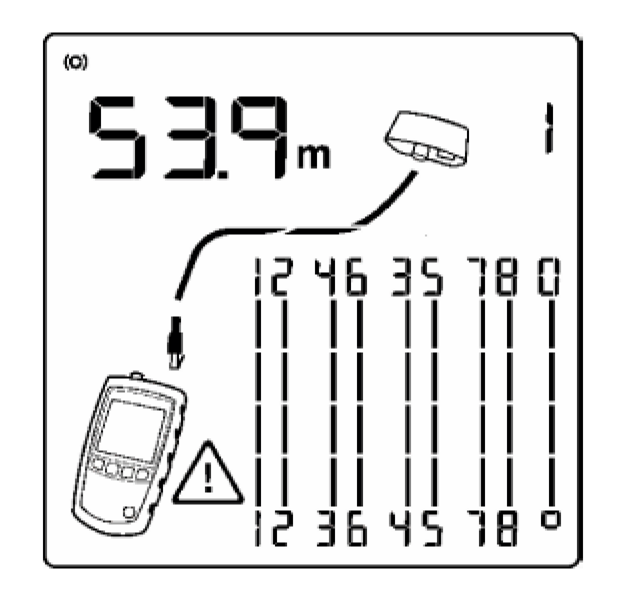


图 8-8　线路跨接

(5) 线对跨接

图 8-9 所示为线对 1、2 和 3、6 跨接，线位号会闪烁来表示故障。这可能是由于接错 568A 和 568B 电缆引起。当然，也可能是专门制作的用于交换机之间连接的交叉线。电缆长度为 32.0m。

(6) 串绕

图 8-10 所示为线对 3、6 和 4、5 存在串绕，串绕的线对会闪烁来表示故障。电缆长度为 75.4m。在串绕的线对中，端到端的连通性正确，但是，所连接的线来自不同线对，如图 8-11 所示。线对串绕会导致串扰过大，因而干扰网络运行。

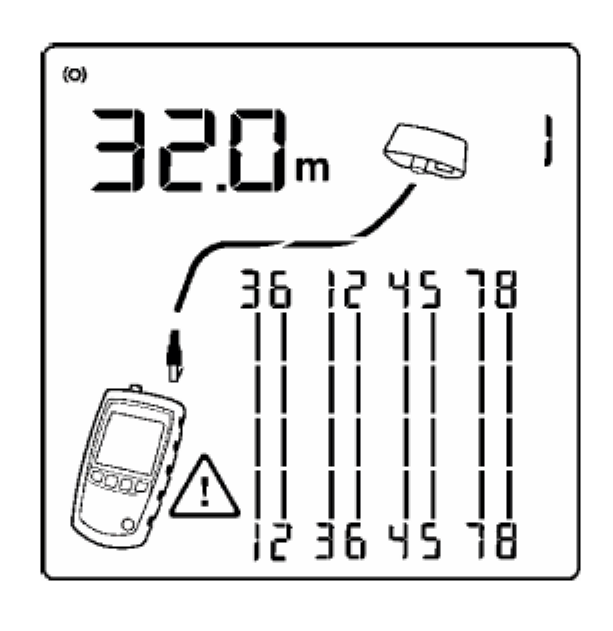


图 8-9　线对跨接

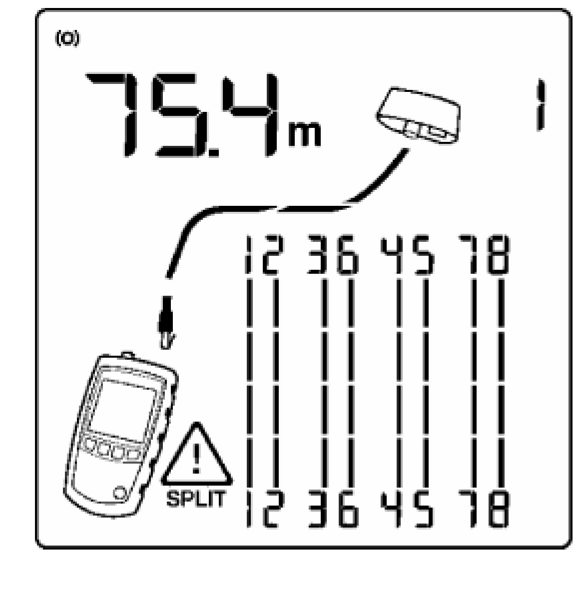


图 8-10　串绕

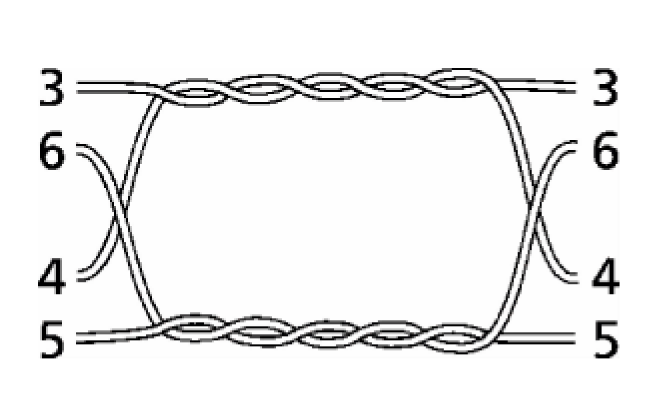


图 8-11　错误线对

小知识：如电话线之类的非双绞线电缆，由于串扰过大，通常会显示为串绕。

3. **水平布线测试**

测试水平布线—配线架至信息插座的连通性时，必须借助于线序适配器才能完成链路测试。

在这里需要使用两根直通跳线，并确认该跳线的连通性完好。使用一根跳线连接配线架欲测试端口和线序适配器；使用另一根跳线连接信息插座（与该配线架端口相对应的端口）与 MicroScanne² 的 RJ-11/45 端口，如图 8-12 所示。

以下测试过程与上述跳线连通性测试相同，故不再赘述。

小技巧：两个人使用无线对讲机在水平布线的两端协同工作，可以大大提高布线测试工作效率。

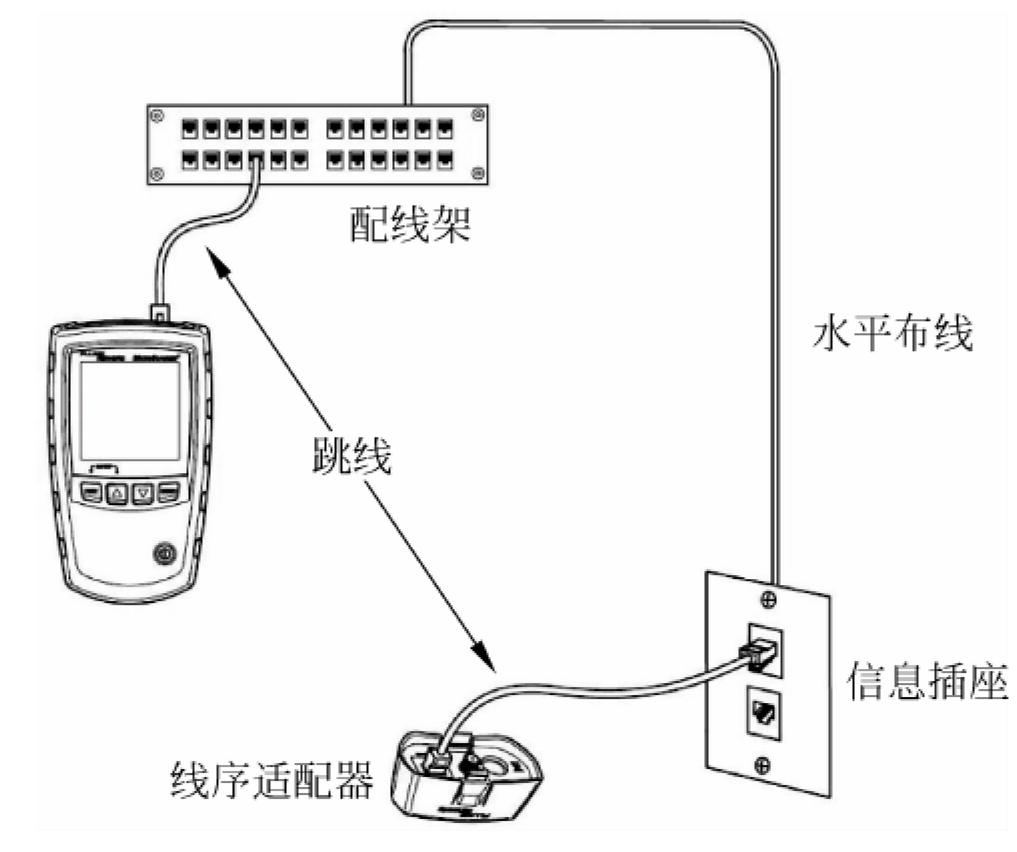


图 8-12　水平布线测试连接方式

4. **整体链路测试**

与测试跳线不同，由于整体链路两端相距较远，不可能同时插入 MicroScanner² 的两个端口测试，所以必须借助于适配器才能完成测试。

将连接计算机和信息插座的跳线从网卡上拔出，插入 MicroScanner² 的 RJ-11/45 端口。然后再将连接配线架和集线设备的跳线从交换机中拔出，插入 MicroScanner² 的线序适配器。

以下测试过程与上述跳线连通性测试相同，故不再赘述。当发现连通性故障时，再逐一测试两端跳线和水平布线。

5. **测试以太网端口**

测试仪能检测现用以太网端口（如图 8-13 所示）和非现用以太网端口（如图 8-14 所示）。

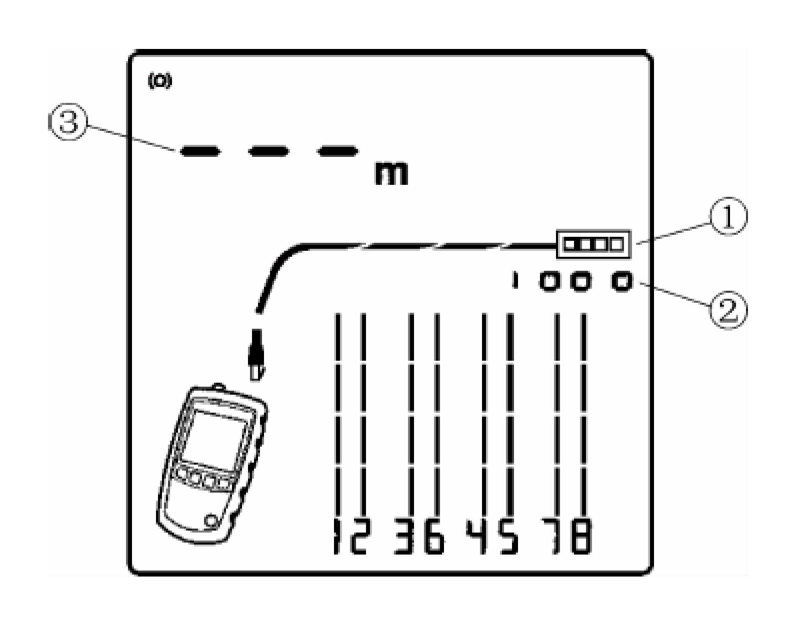


图 8-13　现用以太网端口

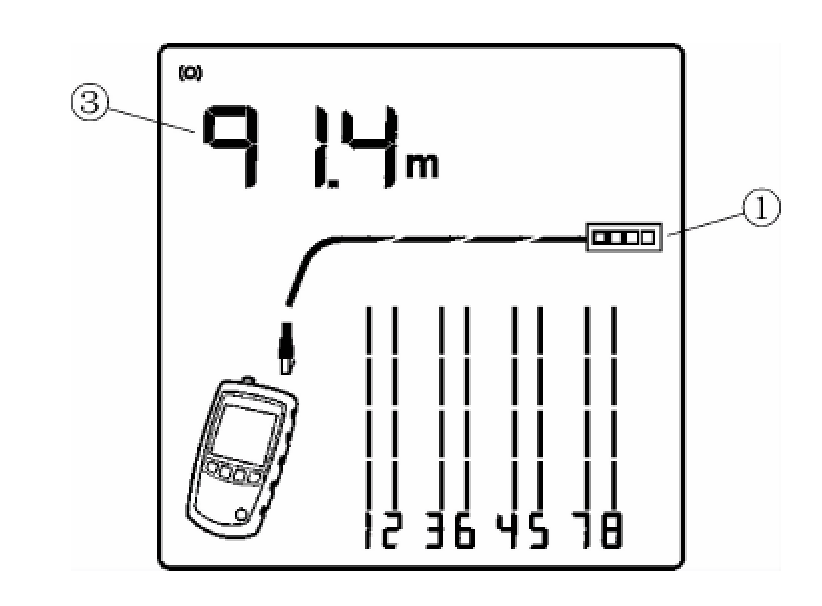


图 8-14　非现用以太网端口

（1）以太网端口图标。

（2）现用 1000Mbps 端口的速率。速率为 10Mbps、100Mbps 或 1000Mbps。示例显示速率为 1000Mbps。如果端口支持多个速率，数字会在各个速率之间循环变换。

（3）电缆长度。如果测试仪无法测量长度，则显示短划号。在端口不能产生反射时会出现这种情况。如果端口的阻抗发生波动或者不同于电缆的阻抗，长度可能会发生不断变化或者明显过高。若有疑问，可将电缆从端口断开，以进行准确的长度测量。

6. 查看单独结果

要查看每个线对的单独结果，可用△键或▽键在屏幕之间移动。在此模式下，测试仪仅连续测试用户正在查看的线对。

图 8-15 所示为线对 1、2 在 29.8 m 处存在短路。图 8-16 所示为线对 3、6 长度为 67.7m，并与线序适配器端连接。

小知识：在单独结果屏幕上，只显示某个线对中接线之间的短路。当存在短路时，远端适配器和未短路接线的线序不显示。

图 8-17 所示为线对 4、5 在 48.1m 处存在开路。开路可能是一根或两根接线。




图 8-15 线对 1、2 短路

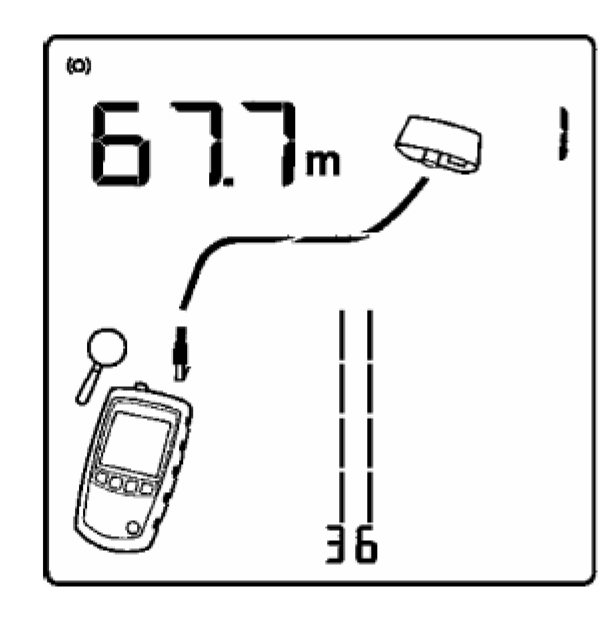


图 8-16 线对 3、6 长度

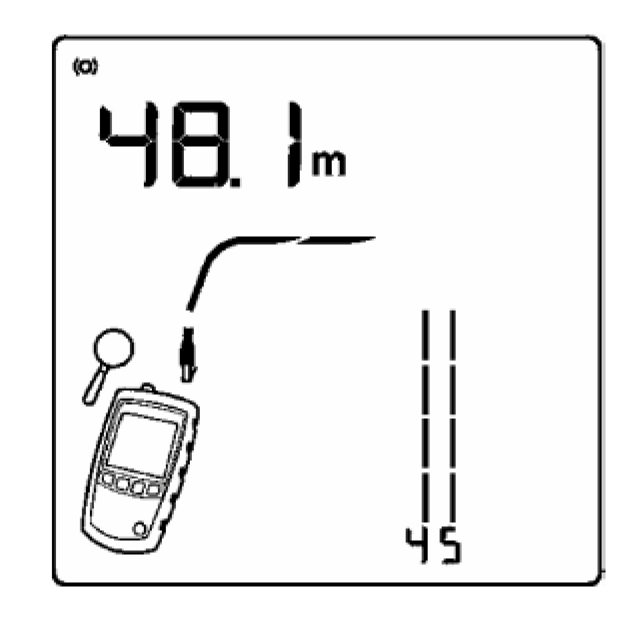


图 8-17 线对 4、5 开路

7. 使用多个远程 ID 定位器

使用多个远程 ID 定位器可帮助识别接插板处的多个网络连接，如图 8-18 所示。画面显示测试仪连接到编号为 3 的远程 ID 定位器端的电缆。

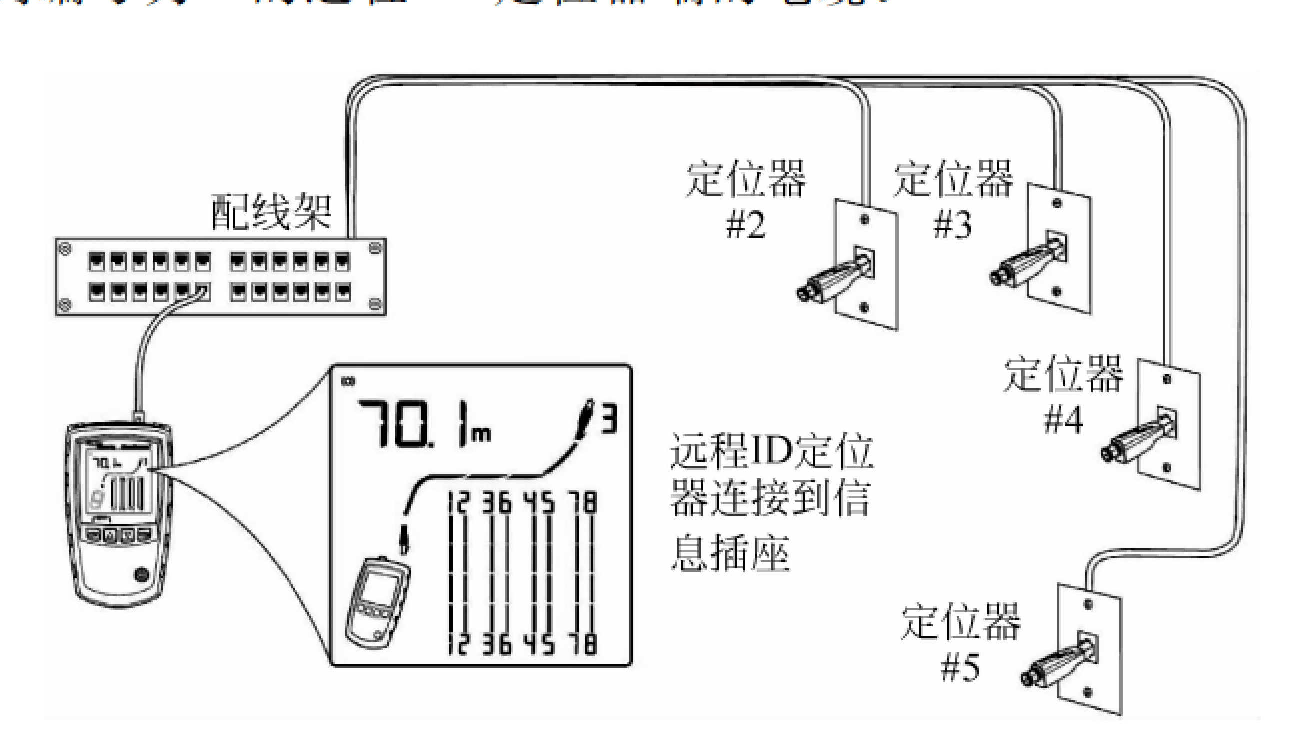


图 8-18 线路定位器

8. 双绞线长度测量

(1) 校准长度测量

测试仪使用一个 NVP 值（名义传播速率）和通过电缆的信号延时来计算长度。测试仪的默认 NVP 值的准确度通常足以验证长度，但是，可通过将 NVP 值调整到指定或实际值来提高长度测量的准确度。默认 NVP 值对双绞线电缆为 70%。

注意：电缆类型、批次和制造商不同，NVP 值也不同。在多数情况下，这些差别较小，可以忽略不计。

(2) 将 NVP 设为指定值

输入由制造商指定的 NVP 值的步骤如下。

① 在启动测试仪时,按下 PORT 键和△键。

② 用△键和▽键来设置 NVP 值。

③ 保存设置值并退出 NVP 模式,将测试仪关闭,然后重新启动。

(3) 测定电缆的实际 NVP 值

可以通过将测得的长度调整到电缆的已知长度来测定电缆的实际 NVP 值。

测定电缆的 NVP 的步骤如下。

① 在启动测试仪时,按下 PORT 键和△键。

② 将已知长度的待测电缆连接到测试仪的双绞线或同轴电缆连接器上。

注意:电缆长度必须不小于 15m(49ft)。如果电缆过短,则会出现"---"来表示长度。为了获得最高的准确度,使用的电缆长度应在 15m(49ft)和 30m(98ft)之间。电缆不可连接任何东西。

③ 在 m 和 ft 之间切换,按 PORT 键。

④ 使用△键和▽键更改 NVP 值,直到测得的长度与电缆的实际长度相同。

⑤ 保存设置值并退出 NVP 模式,将测试仪关闭,然后重新启动。

8.2.2 简易网线测试仪

除在网络管理中心购买 Fluke MircoScanner² 外,在各部门间有时也需要测试网络链路,如果也购买 Fluke MircoScanner²,对于网络预算而言显然是不可接受的,此时,则可以购买廉价的网线测试仪。这里以上海三北的"能手"计算机网络电缆测试仪为例,如图 8-19 所示,虽然功能差一些,但价格非常便宜,只要几十元人民币,且用于网线的连通性测试绰绰有余。

将网线两端的水晶头分别插入主测试仪和远程测试端的 RJ-45 端口,将开关开至 ON (S 为慢速挡),主机指示灯从 1~8 逐个顺序闪亮,如图 8-20 所示。

若连接不正常,按下述情况显示。

(1) 当有一根导线断路,则主测试仪和远程测试端对应线号的灯都不亮。

(2) 当有几条导线断路,则相对应的几条线的显示灯都不亮,当导线少于两根线连通时,灯都不亮。

(3) 当两头网线乱序,则与主测试仪端连通的远程测试端的线号对应的显示灯亮,如图 8-21 所示。



图 8-19 "能手"计算机网络电缆测试仪

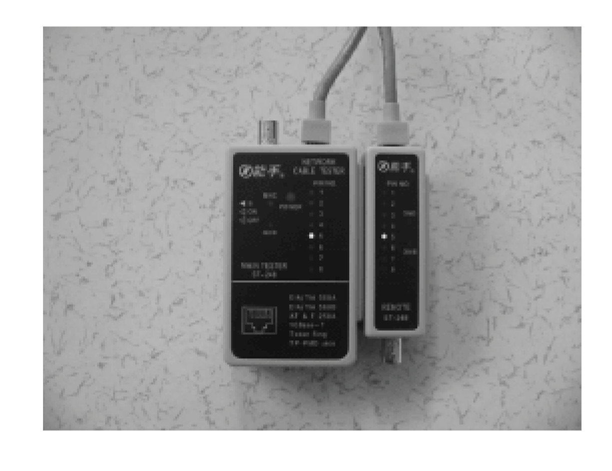


图 8-20 开始测试



图 8-21 乱序

(4) 当导线有两根短路时,则主测试器显示不变,而远程测试端显示短路的两根线灯都亮。若有 3 根以上(含 3 根)短路时,则所有短路的几条线号的灯都不亮。

8.2.3 光纤链路测试

Fluke DTX 系列电缆认证分析仪(如图 8-22 所示)是一款既可满足当前要求又面向未来技术发展的高技术测试平台,被广泛应用于网络布线系统测试。另外,Fluke DTX 系列电缆认证分析仪还可以测试双绞线的布线系统性能。

1. 测试连接

开始双绞线或光纤性能测试前,应当将 Fluke DTX 测试仪连接至欲测试的网络链路中。图 8-23 所示为光纤链路测试模块,图 8-24 所示为双绞线链路测试模块。



图 8-22 Fluke DTX 系列电缆认证分析仪



图 8-23 光纤链路测试模块



图 8-24 双绞线链路测试模块

注意:测试不同类型的链路应当使用不同的模块。

(1) 光纤链路连接

测试光纤链路时,Fluke DTX 测试仪的连接如图 8-25 所示。

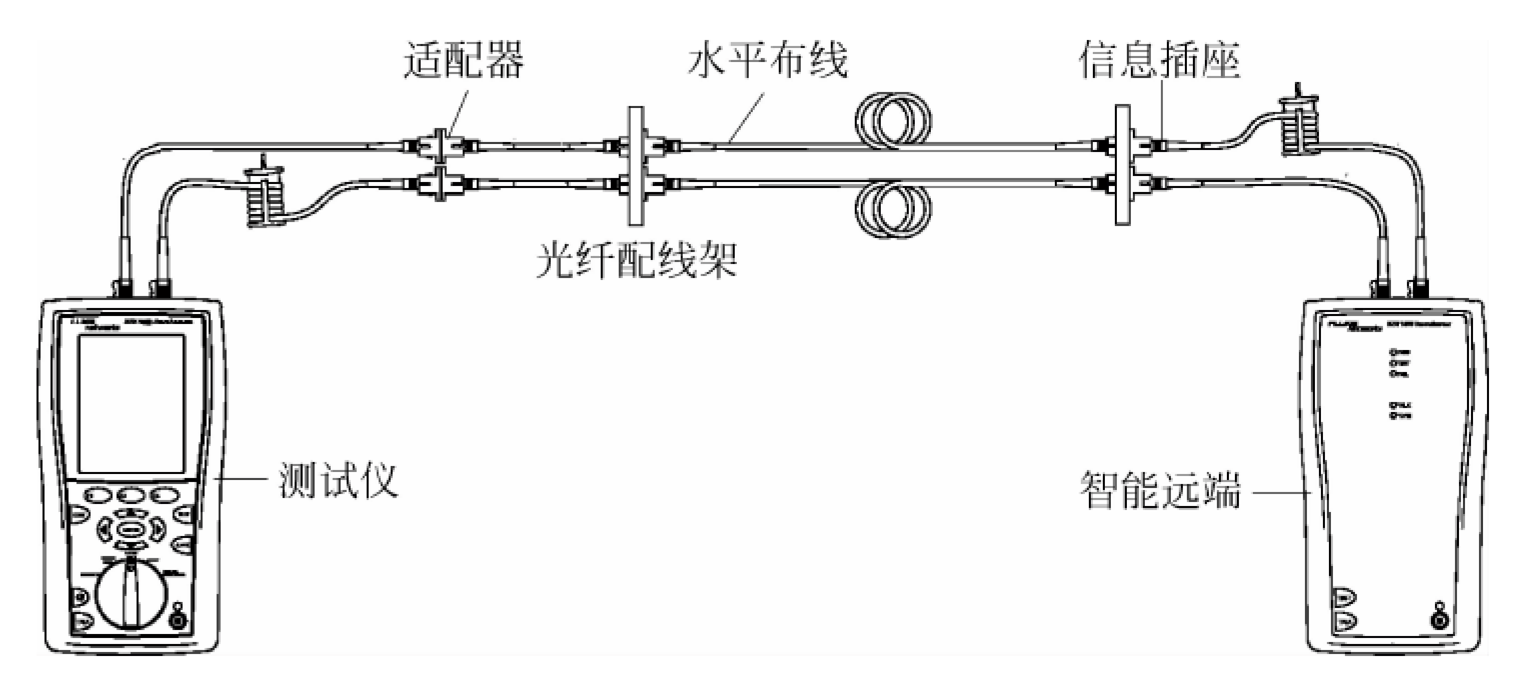


图 8-25 光纤链路测试连接

(2) 双绞线链路连接

测试双绞线水平布线链路时,Fluke DTX 测试仪的连接如图 8-26 所示。

测试双绞线整个通道链路时(包括跳线),Fluke DTX 测试仪的连接如图 8-27 所示。

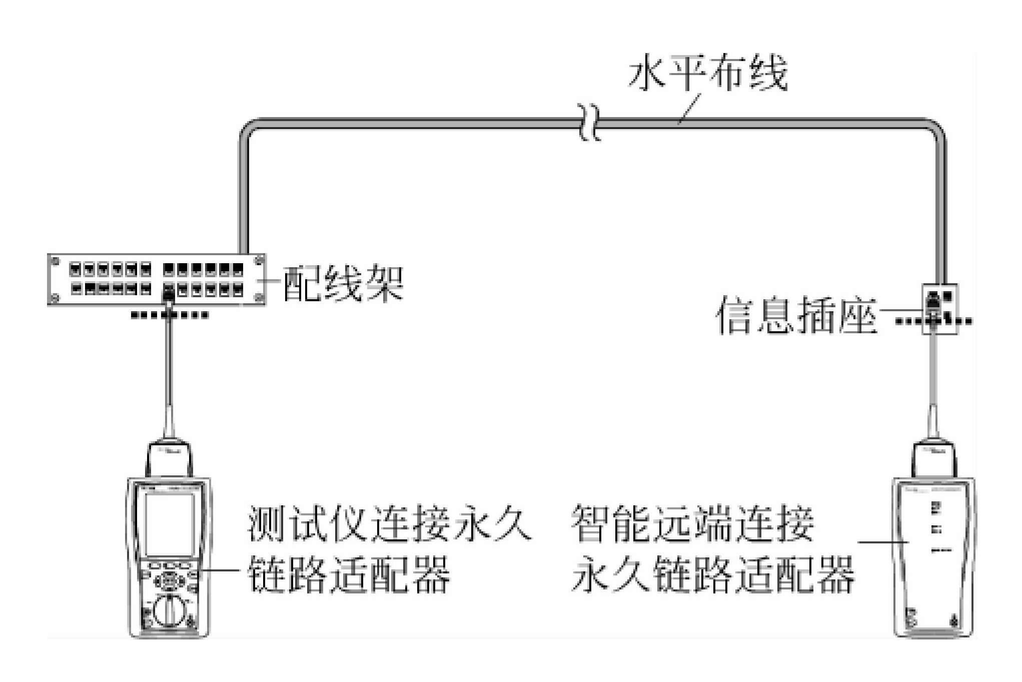


图 8-26 双绞线链路测试连接

2. 设备设置

DTX 为专为快速测试和诊断而设置的通俗易懂的用户界面,使测试前的设备设置工作更加简单,即使是没有经过任何相关培训的普

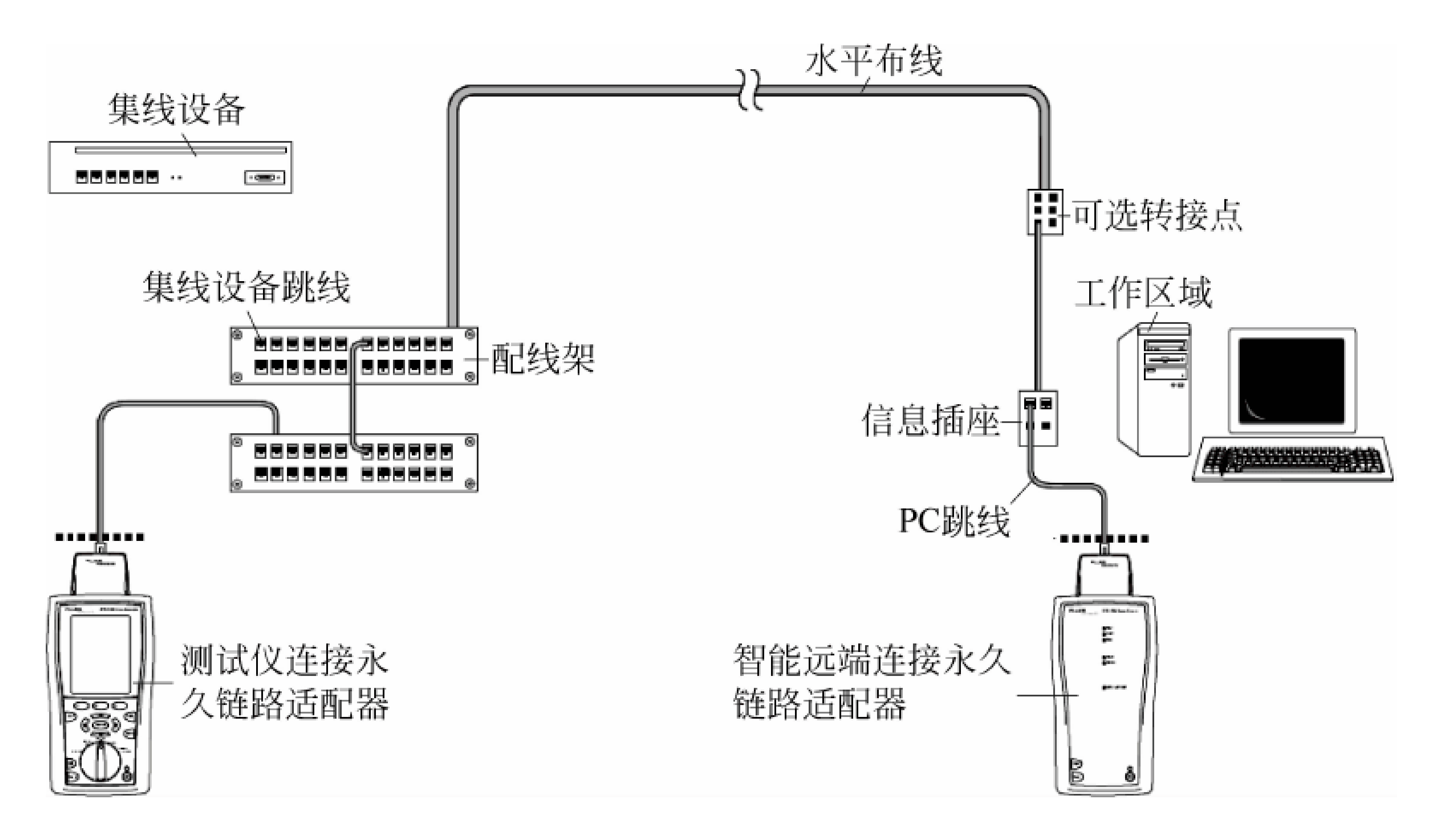


图 8-27　双绞线通道测试连接

通管理员也可简单上手。通常情况下应用于不同的测试环境时需要随时设定不同的参数，但是用户也可以使用附带的管理软件 LinkWare 预先设置好，从而可以留出更多时间用于测试工作。

首先将旋转开关调节至 Setup（设置）位置，并使用测试仪控制面板上的方向选择按钮选择“仪器设置值”选项，此时屏幕上会显示图 8-28 所示的界面。

按 ENTER 键即可进入设置页面，共有 4 个选项供用户自定义，即是否保存测试结果、Fluke Networks 语言、长度单位和是否播放声音。通过定位键中的左右方向调节按钮即可相互切换，在某项功能设置页面中可以使用上下方向调节按钮选择设置结果。图 8-29 所示的是默认显示的是否保存测试结果的界面。

确认选择的设置之后，按 ENTER 键即可保存设置结果。

3. 双绞线测试

1）双绞线设置

首先将旋转开关调节至 Setup 位置，并在显示界面中选择“双绞线”选项，按 ENTER 键，进入图 8-30 所示的双绞线设置界面。



图 8-28　进入仪器设置界面



图 8-29　设置过程



图 8-30　双绞线设置

从图中可以看出，还需要对被测试网络中“线缆类型”、“测试极限值”、NVP 和“插座配置”等选项进行相应的设置，其中最重要的是前两项的设置。

（1）线缆类型。DTX CableAnalyzer 可以广泛支持目前局域网布线中使用的各种屏蔽双绞线和非屏蔽双绞线（STP、FTP、SSTP 和 UTP），选择“线缆类型”选项后，进入图 8-31 所示的“线缆类型”界面，用户可以根据被测试的网络线缆类型选择 UTP、FTP 和 SSTP 等。另外，用户还可以根据所采用线缆的制造商进行选择。

（2）测试极限值。为测试任务选择适当的测试极限值，以便得到更精确的测试结果。在双绞线设置界面中调节选择键，使“测试极限值”高亮度显示，然后按 ENTER 键进入图 8-32 所示的“测试极限值”设置界面。DTX 包含了许多由标准团体制定的测试极限值，如 TIA、ISO、EN、AuS/NZ 和许多应用领域的专用测试极限值。

另外，DTX 还会自动保存最近测试过程中设置的测试极限值，如果需要对当前网络进行反复测试，则可以选择该选项，省去重复设置的麻烦。选择“上次使用”选项，并按 ENTER 键之后进入图 8-33 所示的界面。DTX 最多可以保存 9 项最近应用的测试极限值，分别按照使用的先后顺序进行排列，最近使用的选项显示在第一行。通过上下调节键可以选择本次想要应用的测试极限值，然后按 ENTER 键即可确认选用。



图 8-31　选择线缆类型



图 8-32　设置测试极限值

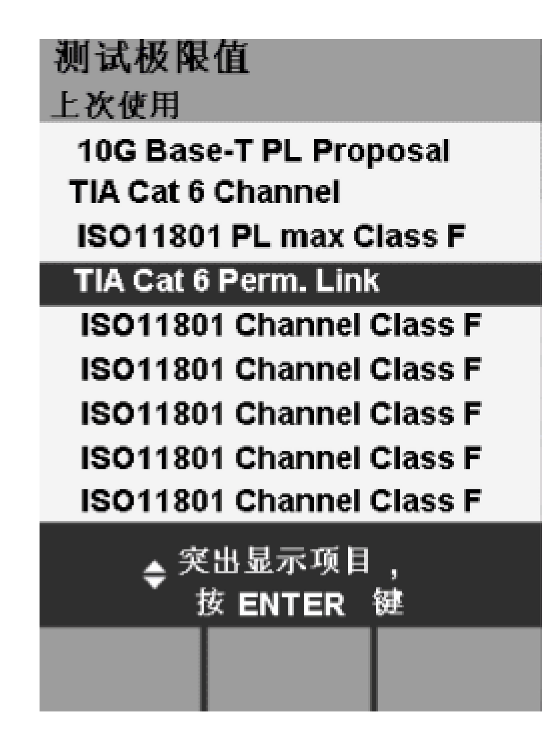


图 8-33　选择原有测试限制

（3）NVP。NVP 表示测试过程中传播的额定速度，通常情况下可以通过测得的传播延迟来计算缆线长度。选定的双绞线类型所定义的默认值代表该特定类型的典型 NVP。如果需要，还可以输入另一个值。增加 NVP 将会相应增加测得的长度。

2）插座配置

输出配置设置值决定测试哪一个缆线对以及将哪一个线对号指定给该线对。要查看某个配置的线序，选择 Outlet Configuration（插座配置）屏幕中的 J Sample（取样）选项。

（1）双绞线自动测试。可以在非常短的时间内完成双绞线自动测试也是 DTX 值得称赞的一个重要功能，例如 DTX 可以在 12s 内完成一个六类双绞线网络的测试工作，并能完整准确地显示出测试结果。双绞线自动测试工作，可以按照如下步骤完成。

① 首先将适用于当前任务的适配器连接至 DTX 测试仪及智能远端，如果在此之前并未设置过双绞线测试选项，则需要先将旋转开关调节至 Setup 位置，完成上述双绞线设置选项，如果已经完成双绞线选项设置（接着“双绞线设置”继续操作）则只需将旋转开关调节至 AUTO TEST（自动测试）位置即可，此时会显示图 8-34 所示的界面，包括当前双绞线设置

的一些详细信息，例如操作员、地点、是否存储绘图数据等。需要注意的是，必须确保智能远端已经同时开启。

提示：“更改介质”按钮是用来快速更改当前测试介质的，例如如果已经安装了光纤模块，则需要按 F1(更换介质)键，确认已经选择了适合当前测试任务的介质类型，本例中应确认选择的是 Twisted Pair(双绞线)选项。

② 按下 DTX 测试仪或智能远端上的 TEST 键即可开始测试，显示图 8-35 所示的界面。测试过程中若想取消测试，按 EXIT 键即可。

小知识：若启动测试过程的同时启动音频发生器，就可以在需要时使用音频探测器，然后才进行连接。信号声也会激活连接布线另一端休眠中或电源已关闭的测试仪。

③ 测试完成后会在屏幕上显示图 8-36 所示的信息，该界面中显示的都是在本次测试过程中接受测试的参数选项和本次测试的具体结果(通过或者失败)。若想查看每一项的详细信息，可以通过上下方向键突出显示被查看项并按 ENTER 键进入。需要注意的是，本例的测试结果是成功的，当测试过程失败时会在 F1 键对应的上方出现一个“错误信息”选项，按 F1 键即可查看，同样按 F2 键和 F3 键可以分别查看上一页和下一页。

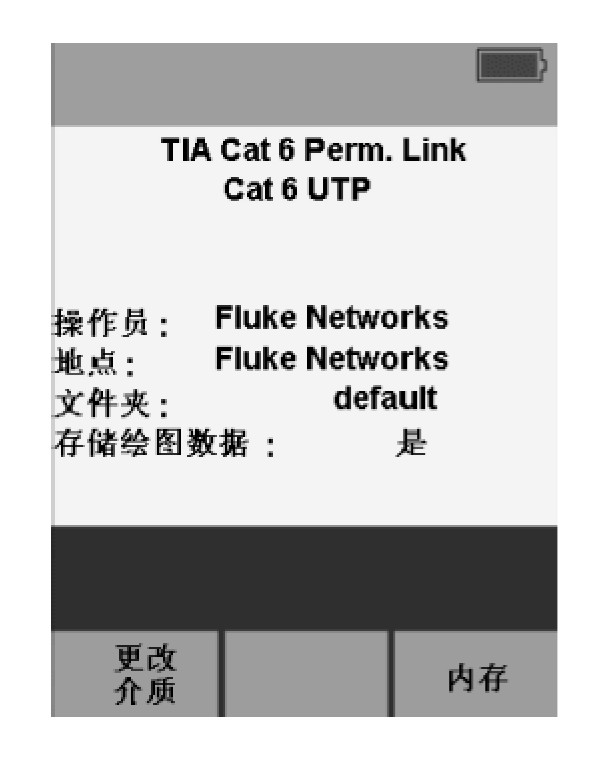


图 8-34 双绞线设置信息



图 8-35 正在测试



图 8-36 测试结果概要

通常情况下，具体测试中可能出现的结果包括以下几种。

- PASS(通过)：显示为绿色，表示所有参数均在极限值设置范围之内。
- PASS *(通过 *)：显示为黄色，表示测试结果中有一个或一个以上的参数准确度在测试用准确度不确定范围内，并在对应的参数前标注蓝色“ * ”，表示该参数勉强可用，但应寻求改善布线安装的方法来消除勉强的性能。
- FAIL *(失败 *)：显示为红色，意义同 PASS * 相同，但是对应参数面前会被标注红色“ * ”，表示该项参数性能接近失败。注意，对于接近失败的测试结果应当视为完全失败来重新统一部署。
- FAIL(失败)：显示为红色，表示测试结果中有一个或者一个以上的参数值超出预先设定的极限值。

④ 为了最后可以查看到完整的测试结果，建议在做其他操作之前先将测试结果保存到 DTX 测试仪的存储设备上，按 SAVE 键显示图 8-37 所示的界面，当前显示的是曾经保存的

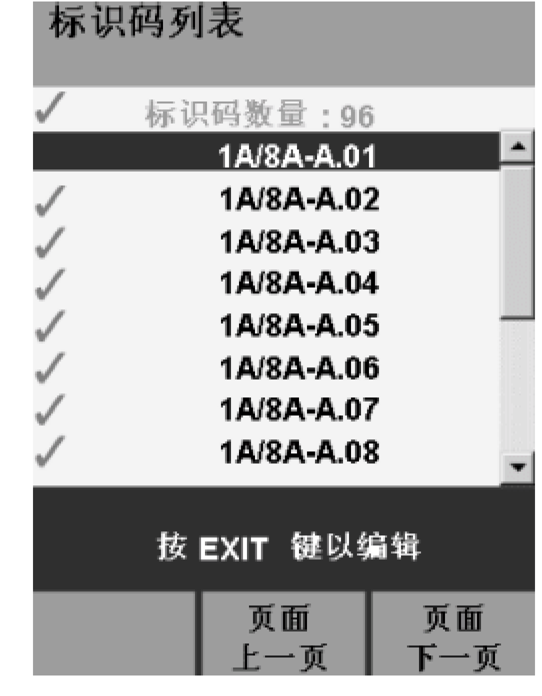


图 8-37 保存测试结果

测试结果。

⑤ 按照提示信息按 EXIT 键显示图 8-38 所示的信息，通过上下左右 4 个定位键选择相应的字符，然后按 ENTER 键确认保存名称。

⑥ 最后再次按 SAVE 键，完成测试结果保存。

(2) 双绞线诊断。DTX 系列产品的诊断功能也是非常强大的，不仅可以完成初装工程的线缆测试工作，还可以在短时间内检测出网络中出现故障的位置。利用 DTX 诊断网络故障省时省力，是同类故障诊断工具速度的两倍以上。通常情况下测试故障网络时会显示图 8-39 所示的诊断结果。

其中诊断参数前面有不同标记，一般故障诊断可能出现的结果包括以下几种。

① 绿色√：表示该参数在预先设定的极限值范围之内。

② 蓝色 i：表示参数已被测量，但选定的测试极限值内没有“通过/失败”极限值。

③ 红色×：表示该参数为通过测试。

④ 蓝色 *：表示通过 *（可参照“双绞线自动测试”中的测试结果）。

⑤ 红色 *：表示失败 *（可参照“双绞线自动测试”中的测试结果）。

按 F1 键即可查看错误信息，如图 8-40 所示。诊断屏幕界面会以图形、图表等通俗易懂的方式显示可能的失败原因及建议用户可采取解决问题的方法。诊断测试失败可能产生一个以上的诊断屏幕，此时可以通过上下左右定位键切换查看。



图 8-38　设置保存名称



图 8-39　故障诊断结果

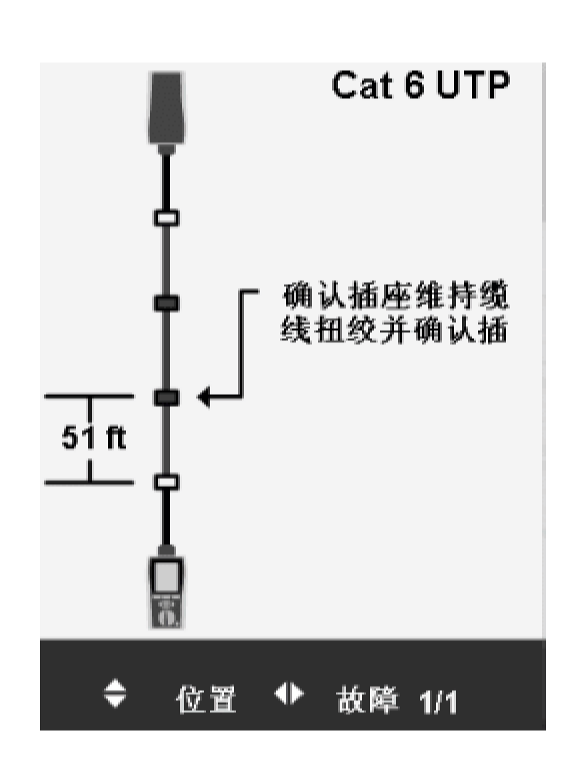


图 8-40　故障信息

另外，从故障信息界面中还可以分析得出导致故障的原因，以及故障位置距离测试仪的大概距离，以便用户迅速确认故障位置，部署相应的排除工作。如果对当前显示的故障分析仍不满意，也可以根据以图形格式表示的标准限制查看故障分析，如图 8-41 所示。通过左右定位键移动光标可以查看到每一时刻状态数据。

4. 光缆测试

光缆由于其自身的一些特性原因，没有双绞线那样灵活自如，但是在远程数据传输或者高可靠性的网络连接环境中主要还是应用光缆，因此光纤测试相对双绞线测试距离一般比较远，所需仪器比较精密。有了 DTX 就不必担心了，因为它同时可以用来测试和诊断光纤网络，并且通过应用独家设计技术大大提高了测试速度。

1) 光纤设置

开始光纤设置之前首先将光纤模块按照安装说明手册正确安装好，然后开启 DTX 电

源，将旋转开关调节至 Setup 位置，并选择"光纤"选项，接着按 ENTER 键即可查看需要设置的选项，如图 8-42 所示，包括光纤类型、测试极限值和远端端点设置 3 项，按照默认顺序依次进行设置即可。

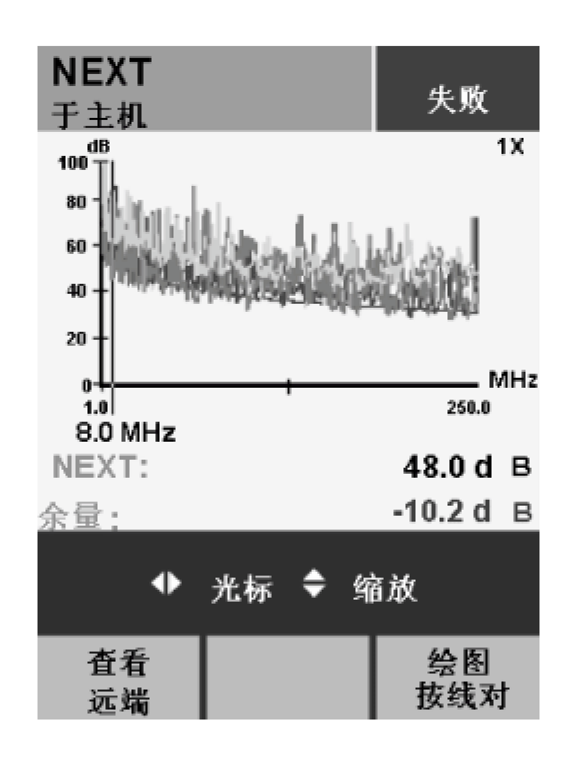


图 8-41　以图形格式显示故障信息



图 8-42　需要设置的光纤选项

（1）光纤类型。即选择适应当前测试任务的光纤类型，根据分类标准的不同分类结果也是多种多样的，DTX 采用了按照传输模式划分、按照波长划分等多种常用分类标准，例如按照传输模式进行划分，可以分为单模光纤和多模光纤。其中多模光纤的光芯比较粗，通常有 50μm 和 62.5μm 两种。由此可见光纤的分类是非常详细的，所以在选择光纤类型过程中应特别慎重。

① 选择"光纤类型"选项后按 ENTER 键，即可显示图 8-43 所示的光纤类型选择页面。在这里用户可以选择通用光纤类型，然后选择对应的光纤型号，也可以根据制造商的不同而选择相应的光纤类型，建议用户选择"通用"选项。

② 选择"通用"选项后按 ENTER 键即可进入详细的光纤类型选择页面，如图 8-44 所示。包括了各种分类标准所产生的分类结果，如 Multimode 62.5、Multimode 50、Singlemode、Singlemode 9μm、Singlemode 18P、Singlemode OSP 和 OF-300 Multimode 62.5 等。



图 8-43　选择光纤类型



图 8-44　选择对应的光纤类型

③ 使用上下方向键可以选择不同的选项，最后按 ENTER 键即可确认保存选择，返回光纤设置界面。

（2）测试极限值。为当前任务设定相应的测试极限值，以保证测试结果的准确性。通过上下方向键选择“测试极限值”选项并按 ENTER 键显示图 8-45 所示的界面。在这里默认显示的是 DTX 测试仪自动保存的最近试用的 9 项测试极限值，按照保存时间的长短依次排列。如果需要对同一任务进行反复测试，则省去了重新设置的步骤，大大提高了测试效率。



图 8-45　曾用测试极限值

（3）远端端点设置。光纤测试远端端点设置共包括 3 种，分别应用于不同的测试任务：用智能远端模式来测试双重光纤布线；用环回模式来测试跳接线与光缆绕线盘；用远端信号源模式及光学信号源模式来测试单独的光纤。

（4）双向。根据当前执行的测试任务决定是否选择双向模式，例如，若当前测试任务是双向测试，则应选择为“是”。在“智能远端”或“环回”模式中启用“双向”测试时，测试仪提示要在测试半途切换测试连接。在每组波长条件下，测试仪可对每根光缆进行双向测量（850 nm/1300 nm，850 nm/1310 nm 或 1310 nm/1550 nm）。

（5）适配器数目和拼接点损耗。输入将在设置参考后被添加至光纤路径的每个方向的适配器及熔接数。如果所选的极限值使用计算的损耗极限值，输入在设置参数后将被添加至光纤路径的适配器数目。拼接点损耗是指每千米损耗、每连接器损耗及每拼接点损耗最大值的极限值，使用计算极限值作为总损耗。

（6）连接点类型。选择用于待测布线的连接器类型，如果未列出实际的连接器类型，可以选择“通用”选项。此设置值仅会影响显示作为基准连接的图表。

（7）测试方法。损耗结果包含设置基准后添加的连接。基准及测试连接可决定将哪个连接包含于结果当中。测试方法决定所含端点连接数的不同，包括 A、B、C 共 3 种。

① 方法 A：损耗结果包含链路一端的一个连接。

② 方法 B：损耗结果包含链路两端的连接。

③ 方法 C：损耗结果不包含链路各端的连接，仅测量光纤损耗。

以上 3 种测试方法只是对于 DTX 测试设备而言的，另外，工业标准中对于相同的测试方法所采用的名称也是不同的，表 8-1 中列出的是 DTX 测试仪标准和四大通用工业标准所采用的 3 种光纤测试方法的对比情况。

表 8-1　DTX 标准名称和四大通用工业标准名称

损耗结果包含的链路端点连接数	DTX 测试仪	TIA/EIA-526-14A（多模）	TIA/EIA-526-7（单模）	IEC 61280-4-1（多模）	IEC 61280-4-2（单模）
1 个连接	方法 A	方法 A	方法 A-2	方法 1	方法 A-2
2 个连接	方法 B	方法 B	方法 A-1	方法 2	方法 A-1
无连接	方法 C	方法 C	方法 A-3	方法 3	方法 A-3

（8）折射率来源（n）。此设置值不会影响损耗的测试结果。它将与测试结果一同保存，以记录用户所用的方法，测试仪使用目前选定的光纤类型（默认值）所定义的折射率（n）或用户值。选定的光纤类型所定义的默认值代表该特定光纤类型的典型值。如果需要，可以输入另一个值。若要决定实际的值，更改折射率，直到测得的长度符合光纤的已知长度。增

加折射率将会增加测得的长度。

2）光纤类型选择

完成光纤设置之后，接着还要选择用于参照测试的光纤类型，在本 DTX 测试仪上设置测试参照非常简单。

（1）首先将旋转开关调节至 SPECIAL FUNCTIONS（特殊参数）位置，此时会显示图 8-46 所示的界面，在这里需要选择“设置基准”选项，其他选项均可保持默认状态。

（2）选择“设置基准”选项后按 ENTER 键，显示图 8-47 所示的界面。设置过程中会出现详细的提示信息帮助用户完成每一步操作，因此即使用户刚刚接触 DTX 也不会感到困难。从该界面中的提示信息可以看出，当前的 DTX 测试仪上只安装了光纤测试模块，所以在“链路接口适配器”选项下面仅有一个“光缆模块”选项可选，如果既安装了光缆模块又连接了双绞线适配器，则为了测试任务的顺利完成就应当确认选择的是“光缆模块”选项。

（3）按 ENTER 键之后，设置基准屏幕画面将会显示用于所选的测试方法（本图为方法 B）的基准连接，如图 8-48 所示，简洁的图形界面更加通俗易懂。清洁测试仪上的连接器及跳接线，连接测试仪及智能远端，然后按 TEST 键。



图 8-46 特殊参数



图 8-47 选择接口适配器



图 8-48 设置参照方式

（4）完成参照设置之后，DTX 将会以两种波长显示选择信息，并且会同时显示选择的测试方法、参照日期和具体时间，如图 8-49 所示。

（5）清洁布线系统中的待测连接器，然后将跳接线连接至布线。DTX 测试仪将显示用于所选测试方法的连接方式，以便进行更精确的测试，如图 8-50 所示。



图 8-49 查看基准

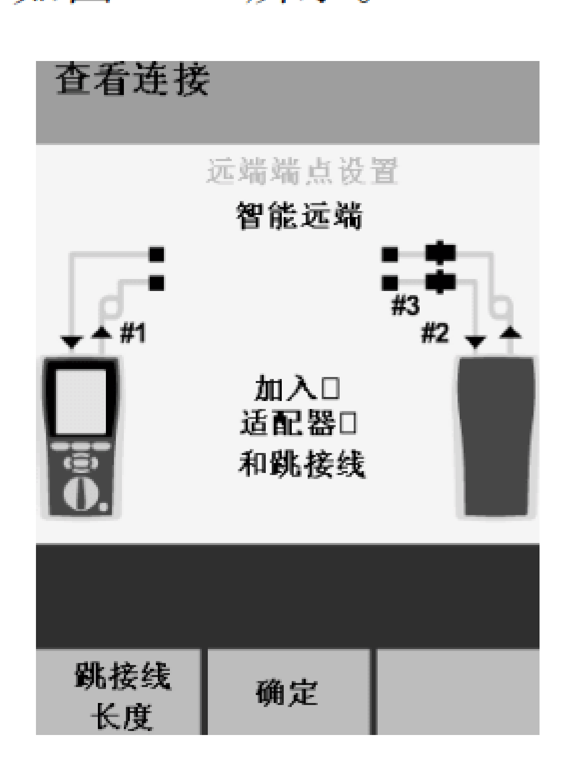


图 8-50 查看连接方式

（6）按 F2 键（确定键），保存所做的设置即可开始光纤自动测试任务。

设置参照基准并不复杂，但需要注意的是，如果在设置基准后将跳接线从测试仪或智能远端的输出端口断开，则需要再次设置基准以确保有效的测量。

3）光纤自动测试

DTX 测试仪的光纤测试模块通过双波长和双向测试使测试速度提高了许多，这两种光纤测试均可在 12s 内完成，是其他同类测试仪器所望尘莫及的。

（1）将旋转开关调节至 AUTOTEST（自动测试）位置，确认介质类型设置为光纤，如果需要切换，按 F1（更换介质）键即可实现。

（2）按 DTX 测试仪或者智能远端的 TEST（测试）键，即可开始测试，显示图 8-51 所示的正在测试界面，按 EXIT 键即可取消测试。

（3）稍等测试完成之后即可显示图 8-52 所示的测试结果，该界面中显示的是输出光纤的详细测试结果，包括输入光纤和输出光纤的损耗情况及长度。

（4）选择某项摘要信息后按 Enter 键即可进入查看其详细结果的界面，如图 8-53 所示。显示结果更为直观，从图中分析可得本次自动测试过程中的实际损耗状态，以及同预先设定的极限值的比较情况。





图 8-51 正在进行光纤测试



图 8-52 测试结果概要



图 8-53 详细测试结果

（5）最后根据提示信息按 Save 键保存测试结果。建议在查看每项测试结果详细信息之前进行保存，以免由于误操作而导致信息丢失。

在光纤自动测试过程中应特别注意，如果选择了双向测试，在测试过程中可能会中途提示切换光纤，即切换适配器的光纤而并非测试仪端口的光纤。

8.3 网络逻辑链路管理

除物理链路会造成网络连接故障外，逻辑链路的不正确配置同样会造成网络连接故障。如所使用的网络协议不正确，IP 地址配置不正确等，此时，则可以使用 Windows 自带的测试工具测试网络链路故障。

8.3.1 IP 网络连通性测试工具——ping

ping 命令是网络中使用频率相当高的命令，经常是在网络不通或传输不稳定时管理员的首选工具。ping 命令内置于 Windows 系统的 TCP/IP 协议中，使用 ICMP 协议来简单地

发送一个数据包并请求应答,接收请求的目的主机再次使用 ICMP 发回同所接收的数据一样的数据。Ping 命令可以清楚地了解每个数据包的发送和接收的往返时间,并报告无响应数据包的百分比,对确定网络是否正确连接、网络连接的状况(包丢失率)是十分有用的。

ping 命令应用非常广泛,不仅可以测试与其他计算机的连通性,还可以用来测试网卡是否安装正确、通过主机名查看 IP 地址等。一般情况下,可以通过“ping IP 地址”或“ping 计算机名”的方法来判断网络连通性。

实例 1:通过 IP 地址测试与其他计算机的连通性

通过 Ping IP 地址的方法可以判断本地计算机与其他计算机的连通性,或者判断对方计算机是否在线等。这是局域网中最常用的操作。

例如,测试与局域网中一个 IP 地址为 192.168.1.77 的计算机是否能够连通。在命令提示符中输入如下命令。

```
ping 192.168.1.77
```

按 Enter 键运行,ping 命令便开始测试,如果能够连通,就会返回一些数值,如时间、TTL 值等,如图 8-54 所示,说明对方计算机当前在线,并且能与该计算机连通。根据所返回的时间和 TTL(生存时间)值,还可以了解到网络的大致性能:时间值越大,说明 Ping 的时间越长,网络延时越大,则网络性能也就越不好;如果时间越小,则说明网络状况越好。

```
命令提示符
Microsoft Windows [版本 6.0.6000]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\czc>ping 192.168.1.77

正在 Ping 192.168.1.77 具有 32 字节的数据:

来自 192.168.1.77 的回复: 字节=32 时间=122ms TTL=128
来自 192.168.1.77 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.77 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.77 的回复: 字节=32 时间<1ms TTL=128

192.168.1.77 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 122ms, 平均 = 30ms

C:\Users\czc>
```

图 8-54 Ping 通 IP 地址

如果运行 ping 命令时返回信息为“请求超时”,则表示不能与该计算机连通,如图 8-55 所示。这种情况说明可能是对方计算机设置了不返回 ICMP 包,或者与对方计算机的网络不通,或测试计算机未在线,也有可能安装了防火墙。

```
命令提示符
C:\Users\czc>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:

请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\czc>
```

图 8-55 不能 Ping 通

实例 2：通过计算机名测试与其他计算机的连通性

如果不知道对方计算机的 IP 地址，只知道对方的计算机名，也可以使用 ping 命令测试，同时，还可以得到对方计算机的 IP 地址。

例如，现在要测试局域网中一台名为 hstjl-PC 计算机的连通性，在命令提示符中输入如下命令。

```
ping hstjl-PC
```

按 Enter 键运行，ping 命令开始测试，如果能够连接，就会返回相应数值，如图 8-56 所示，说明与该计算机的连接正常。在返回值中，还会显示对方计算机的 IP 地址，即 192.168.1.229。

```
命令提示符
^C
C:\Users\czc>ping hstjl-PC

正在 Ping 192.168.1.229 具有 32 字节的数据:

来自 192.168.1.229 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.229 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.229 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.229 的回复: 字节=32 时间=12ms TTL=128

192.168.1.229 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 12ms, 平均 = 3ms

C:\Users\czc>
```

图 8-56　Ping 计算机名

如果在 Ping 计算机名时返回“Ping 请求找不到主机 hsczc。请检查该名称，然后重试”信息，则说明网络中没有此计算机名的计算机，或者是无法与该计算机连通，也可能是本地计算机没有正确接入网络，如图 8-57 所示。

```
命令提示符
C:\Users\czc>ping hsczc
Ping 请求找不到主机 hsczc。请检查该名称，然后重试。

C:\Users\czc>
```

图 8-57　未检查到主机名

实例 3：测试与 Internet 的连通性

用户在浏览网页时，经常会遇到网页不能正常打开的情况。此时可以使用 ping 命令检查本地计算机到 Internet 的连通性，同时也可以获得该网站的 IP 地址。

在返回的结果中，包括所测试网站的 IP 地址及连通信息等。说明可以解析域名并与该网站连通。

提示：有许多网站设置了不返回 ICMP 包，在使用 ping 命令时也会返回“请求超时”的消息，因此，测试时应多 Ping 几个网站。如果此时仍然可以解析出该网站的 IP 地址，说明本地计算机可以连接 DNS 服务器。如果网络中没有专用的 DNS 服务器，则说明计算机可以上网。

在测试与 Internet 的连通时，如果网站禁止 Ping 入，则在命令行提示符窗口中提示“请求超时”信息，但是可以获得该网站 IP 地址 202.108.22.43，如图 8-58 所示。

打开 IE 浏览器，在地址栏中输入网站的 IP 地址 202.108.22.43，运行直接打开网站，如图 8-59 所示。



图 8-58 网站禁止 Ping 入



图 8-59 百度网站首页

实例 4：测试服务器或网络设备的性能

如果欲查看网络中某台服务器或设备的性能如何，也可以通过长时间不断地 Ping 来查看丢包现象，从而判断对方设备的性能。

在命令提示符中输入如下命令。

```
ping 192.168.100.2 -t
```

按 Enter 键运行，ping 命令便会开始不间断地 Ping 该 IP 地址，如图 8-60 所示。从该图中可以看出，经常出现与该 IP 地址的不能连通的情况，说明该服务器或网络设备并不稳定。

```
命令提示符
C:\Users\czc>ping 192.168.100.2 -t

正在 Ping 192.168.100.2 具有 32 字节的数据:

来自 192.168.100.2 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=23ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=1ms TTL=128
请求超时。
请求超时。
请求超时。
来自 192.168.100.2 的回复: 字节=32 时间=8ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
请求超时。
请求超时。
```

图 8-60 测试服务器或设备性能

提示：ping 命令加上-t 参数运行后，会一直 Ping 下去，不会自动停止，需使用 Ctrl+C 键手动停止。

实例 5：测试所发出的测试包的个数

在默认情况下，Ping 只发送 4 个数据包，通过-n count 命令定义发送的个数，对衡量网络的稳定性很有帮助，例如测试发送 10 个数据包的返回平均时间、最快时间和最慢时间分别是多少。

在命令提示符窗口中输入命令。

```
ping -n 10 192.168.100.2
```

按 Enter 键运行，如图 8-61 所示，在给 192.168.100.2 发送 10 个数据包的过程中，返回了 10 个，丢失为 0。在这 10 个数据包当中返回速度最短为 0ms，最长为 43ms，平均速度为 4ms。

```
命令提示符
C:\Users\czc>ping -n 10 192.168.100.2

正在 Ping 192.168.100.2 具有 32 字节的数据:
来自 192.168.100.2 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间=43ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.100.2 的回复: 字节=32 时间<1ms TTL=128

192.168.100.2 的 Ping 统计信息:
    数据包: 已发送 = 10, 已接收 = 10, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 43ms, 平均 = 4ms

C:\Users\czc>
```

图 8-61　测试所发出的测试包的个数

实例 6：定义 echo 数据包大小

在默认的情况下，Windows 系统的 ping 命令发送的数据包大小为 32B，用户也可以自己定义其的大小，但最大只能发送 65500B。

在命令提示符窗口中输入命令。

```
ping -l 1000 -t 192.168.100.2
```

按 Enter 键运行，如图 8-62 所示。这样就会不停地向 192.168.100.2 计算机发送大小为 1000B 的数据包。直至用户按 Ctrl+C 键停止。

```
命令提示符
C:\Users\czc>ping -l 1000 -t 192.168.100.2

正在 Ping 192.168.100.2 具有 1000 字节的数据:
来自 192.168.100.2 的回复: 字节=1000 时间=3ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=2ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=13ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=2ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=2ms TTL=128
来自 192.168.100.2 的回复: 字节=1000 时间=1ms TTL=128
```

图 8-62　定义 echo 数据包大小

8.3.2 知识链接：ping 命令介绍

1. ping 命令的应用

造成网络性故障的原因有很多，要解决网络连接性故障，需逐步排除各个环节，例如本地网卡、网络协议、本地网络电缆以及到远程计算机的连接等，这些均可使用 ping 命令完成。

(1) 测试网卡

如果计算机与不能与其他计算机或 Internet 正常连接，首先需要检查本地网卡是否正常。网卡可能会因为驱动程序安装不正常、没有安装必需的通信协议等情况造成不能连接网络。此时，可使用"ping 本地 IP 地址"或者"ping 127.0.0.1"进行测试，通过测试可以得到以下信息。

① 是否正确安装了网卡。如果测试成功，说明网卡没有问题；如果测试不成功，说明该网卡驱动程序或 TCP/IP 协议没有正常安装。

检查网卡驱动步骤为：打开"设备管理器"窗口，展开"网络适配器"目录，查看网卡是否有一个黄色的"!"。如果有，就需重新安装驱动程序。

提示：127.0.0.1 是本地网卡的默认回环地址，无论网卡中是否分配了 IP 地址，该地址都会存在，且仅在本地计算机中有效，在网络中无效。

② 是否正确安装了 TCP/IP 协议。如果测试成功，说明网卡 TCP/IP 协议没有问题。如果不成功并且网卡驱动程序安装正常，则应检查本地网卡的"本地连接"属性，查看是否正确安装了 TCP/IP 协议。

③ 是否正确配置了 IP 地址和子网掩码。如果"ping 127.0.0.1"成功，但"ping 本地 IP 地址"不成功，说明没有正确配置 IP 地址。应打开本地网卡的"本地连接"属性窗口，检查 IP 地址和子网掩码是否设置正确，并进行正确配置。

(2) 测试局域网连接

通过 Ping 局域网内其他计算机或服务器的计算机名或 IP 地址，可测试网络(或同一 VLAN)的连接是否正常。

① 检测 IP 地址和子网掩码设置是否正确。如果局域网内的计算机 ping 不通，则应检查网络连接的 IP 地址和子网掩码配置是否正确。

② 确认网络连接是否正常。如果 IP 地址和子网掩码设置成功，但仍 ping 不通，应当对网络设备和通信介质逐段测试、检查和排除。

(3) 测试与远程主机的连接

通过 ping 命令可以测试与远程主机的连接是否正常，尤其是与 Internet 的连接。该测试可通过 Ping 远程主机的 IP 地址或域名来判断网络中的故障。

① 确认是否能连接 Internet。如果计算机不能浏览网页，可以 ping 网站域名，如果能 Ping 通，说明计算机与 Internet 连接正常，请检查本地 DNS 服务或系统故障。如果不能 Ping 通，可能是对方网站没有运行，或本地计算机根本不能连接 Internet，应检查本地网关或服务器故障。

② 确认 DNS 服务器设置是否正常。如果使用 ping 命令可以 ping 通 Internet 上的 IP 地址，但打不开网页，则可能是 DNS 服务器设置有问题，Ping 本地 DNS 服务器确认是否能正常连接，并在网络连接属性中检查 DNS 服务器设置。

③ 确认本地 Internet 连接是否正常。如果与任何一个主机的连接都超时，或丢包率都非常高，则应当与 ISP 共同检查 Internet 连接，包括线路、Modem 和路由器等多方面的设置。

2. ping 命令参数

ping 命令的功能非常强大，除上述功能外，若配合相应的参数使用，还可实现更多的功能。语法格式如下。

```
ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s Count] [{-j HostList | -k
HostList}] [-w Timeout] [-R] [-R] [-S SrcAddr] [-4] [-6] TargetName
```

各参数说明如下。

(1) -t：向目的地持续发送回响请求信息。

(2) -a：对目的地 IP 地址进行反向名称解析。如果解析成功，Ping 将显示相应的主机名。

(3) -n Count ：定义用来测试所发出的测试包的个数，默认值为 4。

(4) -l Size：指定发送的回响请求消息中"数据"字段的长度(以字节为单位)。默认值为 32，Size 的最大值是 65527。由于过大的数据包会占用大量的带宽，因此，曾被黑客作为攻击服务器的一种手段。

(5) -f：指定发送的"回显请求"中其 IP 标头中的"不分段"标记被设置为 1(只适用于 IPv4)。"回显请求"消息不能在到达目标的途中被路由器分段。

(6) -i TTL：指定回响请求消息的 IP 数据头中的 TTL 值。其默认值是主机的默认 TTL 值，TTL 的最大值为 255。

(7) -v TOS：指定发送的"回显请求"消息的 IP 标头中的"服务类型"(TOS)字段值(只适用于 IPv4 可用)。TOS 的值是 0～255 之间的十进制数，默认值是 0。

(8) -r Count：指定 IP 标头中的"记录路由"选项，用于记录由"回显请求"消息和相应的"回显请求"消息使用的路径(只适用于 IPv4)。Count 的最小值为 1，最大值为 9。

(9) -s Count：指定 IP 数据头中的"Internet 时间戳"选项，用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。Count 的最小值是 1，最大值是 4。

(10) -j HostList：指定"回显请求"消息对于 HostList 中指定的中间目标集在 IP 标头中使用"稀疏来源路由"选项(只适用于 IPv4)。使用稀疏来源路由时，相邻的中间目标可以由一个或多个路由器分隔开。

(11) -k HostList：指定"回显请求"消息对于 HostList 中指定的中间目标集在 IP 标头中使用"严格来源路由"选项(只适用于 IPv4)。

(12) -w Timeout：指定等待回响应答消息响应的时间(以 ms 计)，该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示"请求超时"的错误消息。默认的超时时间为 4000ms(4s)。

(13) -4：指定将 IPv4 用于 Ping。不需要用该参数识别带有 IPv4 地址的目标主机。仅需要它按名称识别主机。

(14) -6：指定将 IPv6 用于 Ping。不需要用该参数识别带有 IPv6 地址的目标主机。仅需要它按名称识别主机。

(15) TargetName：指定目标主机的名称或 IP 地址。

3. 常见的出错信息

用户在使用 ping 命令诊断网络故障过程中，经常会遇到一些错误提示信息，这些错误

信息正是排除故障的重要突破口。

(1) Unknown host

Unknown host(不知名主机),表示该远程主机的名字不能被命名服务器转换成 IP 地址。故障原因可能是命名服务器有故障,或者其名字不正确,或者网络管理员的系统与远程主机之间的通信线路有故障。

(2) Network unreachable

Network unreachable(网络不能到达),表示本地系统没有到达远程系统的路由,可用 netstat -rn 检查路由表来确定路由配置情况。

(3) No answer

No answer(无响应),表示远程系统没有响应。这种故障说明本地系统有一条到达远程主机的路由,但却接收不到发回的任何分组报文。故障原因可能是远程主机没有工作、本地或远程主机网络配置不正确、本地或远程的路由器没有工作、通信线路有故障或者远程主机存在路由选择问题。

(4) Timed out

Timed out(超时),表示与远程主机的链接超时,数据包丢失。故障原因可能是本地主机到路由器的连接问题、路由器不能通过,也可能是远程主机无响应,远程主机禁 Ping 或者死机。

8.3.3 路径信息提示工具——pathping

pathping 命令提供有关在源和目标之间的中间跃点处,网络滞后和网络丢失的信息。pathping 命令在一段时间内将多个回响请求消息发送到源和目标之间的各个路由器,然后根据各个路由器返回的数据包计算结果。因为 Pathping 可以表示在任何特定路由器或链接处的数据包的丢失程度,所以根据这些信息可以确定存在网络问题的路由器或子网。

实例 1:显示本地计算机和服务器之间的路径信息

在命令提示符窗口中输入如下命令。

```
pathping -n www.tsinghua.edu.cn
```

按 Enter 键运行,显示图 8-63 所示的运行结果。

```
命令提示符
C:\Users\czc>pathping -n www.tsinghua.edu.cn

通过最多 30 个跃点跟踪
到 www.d.tsinghua.edu.cn [166.111.4.100] 的路由:
  0  192.168.1.78
  1  192.168.1.1
  2  211.82.216.136
  3  202.206.233.133
  4  202.206.233.6
  5  202.112.53.197
  6  202.127.216.161
  7  202.112.53.170
  8  202.112.38.74
  9  59.66.2.1
 10  59.66.2.18
 11     *        *        *
正在计算统计信息,已耗时 250 秒...
            指向此处的源    此节点/链接
跃点  RTT    已丢失/已发送 = Pct  已丢失/已发送 = Pct  地址
  0                                           192.168.1.78
                                0/ 100 =  0%   |
  1    5ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                0/ 100 =  0%   |
  2    7ms     0/ 100 =  0%     0/ 100 =  0%  211.82.216.136
                                0/ 100 =  0%   |
  3   26ms     0/ 100 =  0%     0/ 100 =  0%  202.206.233.133
                                0/ 100 =  0%   |
```

图 8-63 显示本地计算机和服务器之间的路径信息

首先显示路径信息，然后将显示消息的繁忙情况，显示时间随着跃点数的变化而变化。在此期间，会从列出的所有路由器及其链接之间收集相关的信息。

在 Address 列中所显示的链接丢失速率（以垂直线 | 表示）表明造成路径上转发的数据包丢失的链路处于堵塞状态。路由器显示的丢失速率（由 IP 地址标识）表明这些路由器可能已经超载。

实例 2：显示连接到远程网关的路径信息

在命令提示符下输入如下命令。

```
pathping -n 192.168.1.1
```

按 Enter 键运行，显示图 8-64 所示的运行结果。

```
命令提示符
C:\Users\czc>pathping -n 192.168.1.1

通过最多 30 个跃点跟踪到 192.168.1.1 的路由

  0  192.168.1.78
  1  192.168.1.1

正在计算统计信息，已耗时 25 秒...
            指向此处的源   此节点/链接
跃点  RTT    已丢失/已发送 = Pct  已丢失/已发送 = Pct  地址
  0                                           192.168.1.78
                                0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1

跟踪完成。

C:\Users\czc>_
```

图 8-64　显示连接到远程网关的提示信息

8.3.4　知识链接：pathping 命令介绍

pathping 命令的语法如下。

```
pathping [-n] [-h MaximumHops] [-g HostList] [-p Period] [-q NumQueries [-w Timeout]
[-i IPAddress] [-4 IPv4] [-6 IPv6][TargetName]
```

各参数说明如下。

（1）-n：阻止 pathping 试图将中间路由器的 IP 地址解析为各自的名称，使用该参数可以加快显示 Pathping 的结果。

（2）-h MaximumHops：在搜索目标（目的）的路径中指定跃点的最大数，默认值为 30 跃点。

（3）-g HostList：指定“回显请求”消息在 IP 标题中使用“稀疏资源路由”选项，该 IP 标题带有 HostList 中指定的中间目标集。

（4）-p Period：指定两个连续的 Pathping 之间的时间间隔（以 ms 为单位）。默认值为 250 毫秒（1/4 秒）。

（5）-q NumQueries：指定发送到路径中每个路由器的“回显请求”消息数。默认值为 100 个查询。

（6）-w Timeout：指定等待应答的时间（以 ms 为单位）。默认值为 3000ms（3s）。

（7）-I IPAddress：指定源地址。

（8）-4 IPv4：指定 Pathping 只使用 IPv4。

（9）-6 IPv6：指定 Pathping 只使用 IPv6。

（10）TargetName：指定目的端，既可以是 IP 地址，也可以是主机名。

注意事项如下。

(1) pathping 命令的参数是区分大小写的。

(2) 为避免网络堵塞,建议以非常慢的速度发送 Pathping 信号。

(3) 为减小突发丢失所造成的影响,发送 Pathping 信号不要过于频繁。

(4) 使用-p 参数时,pathping 命令将单独发送到各个中间跃点。因此,向同一跃点发送 pathping 命令的时间间隔为 Period 乘以跃点数。

(5) 使用-w 参数时,可以同时发送多个 pathping 命令。因此,Timeout 参数中指定的时间间隔不受 Pathping 之间等待的 Period 参数指定的时间间隔的限制。

(6) 只有 Internet 协议(TCP/IP)在网络连接中安装为网络适配器属性的组件时,该命令才可用。

8.3.5 测试网络路由路径——tracert

tracert 命令是 Windows 操作系统自带的命令,该命令通过递增"生存时间"(TTL)的值将 Internet 控制消息协议(ICMP)回应数据包或 ICMPv6 消息发送给目标,可以确定到达目标主机的路径。路径将以列表形式显示,其中包含源主机与目标主机之间路径中路由器的近侧路由器接口。

tracert 命令通过跟踪目标主机的方式,确定到达目标主机所需的路径。当网络出现故障时,使用 Tracert 命令可以确定出现故障的具体位置,找出在经过哪个路由时出现了问题,从而使网络管理员缩小排查范围,因此也是网络故障排除过程中常用的一款小工具。

例如,现在要查看到网站 www. tsinghua. edu. cn 所经过的路由及使用时间,在命令提示符中输入如下命令。

```
tracert www.tsinghua.edu.cn
```

按 Enter 键运行,显示图 8-65 所示的运行结果。默认状态下,tracert 命令可以显示 30 条记录。

```
命令提示符

C:\Users\czc>tracert www.tsinghua.edu.cn

通过最多 30 个跃点跟踪
到 www.d.tsinghua.edu.cn [166.111.4.100] 的路由:

  1    28 ms     2 ms     1 ms  192.168.1.1
  2    19 ms     8 ms     3 ms  211.82.216.136
  3    14 ms    13 ms    23 ms  202.206.233.133
  4    12 ms    12 ms    15 ms  202.206.233.6
  5    32 ms    44 ms    20 ms  202.112.53.197
  6    19 ms    43 ms    16 ms  202.127.216.161
  7    16 ms    57 ms    62 ms  202.112.53.170
  8    36 ms    44 ms    39 ms  pku1.cernet.net [202.112.38.74]
  9    35 ms    58 ms    47 ms  th002001.ip.tsinghua.edu.cn [59.66.2.1]
 10    35 ms    67 ms    80 ms  th002018.ip.tsinghua.edu.cn [59.66.2.18]
 11     *        *        *     请求超时。
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14    47 ms    71 ms    95 ms  www.tsinghua.edu.cn [166.111.4.100]

跟踪完成。

C:\Users\czc>
```

图 8-65 跟踪路由

当 ICMP 数据包从本地计算机经过多个网关传送到目的主机,tracert 命令可以跟踪数据包使用的路由(路径),但并不能保证或认为数据包总遵循这个路径。tracert 是一个执行速度比较慢的命令,每经过一个路由器大约需要 15 秒钟。

注意:在使用 tracert 命令检测网络的过程中,很可能会遇到 Request timed out 的提示

信息，出现这种情况，可能是由于当时网络稳定性差，也可能是由于所到达的路由器设置问题。如果连续 4 次都出现该提示信息，说明遇到的是拒绝 Tracert 命令访问的路由器。

8.3.6 知识链接：tracert 命令介绍

tracert 命令的语法参数如下。

tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [-R] [-S SrcAddr] [-4] [-6] TargetName

各参数说明如下。

(1) -d：防止 tracert 命令试图将中间路由器的 IP 地址解析为计算机名称。可加速显示 Tracert 的结果。

(2) -h MaximumHops：指定搜索目标主机的路径中存在的跃点(路由器)的最大数。默认值为 30。

(3) -j HostList：指定回应请求消息将 IP 报头中的松散源路由选项与 hostlist 中指定的中间目标集在一起使用。注意，只有跟踪 IPv4 的目标地址时才使用该参数。

(4) -w Timeout：指定等待 Request timed out 消息或正常回应消息的时间(以 ms 为单位)。如果在限定时间内未收到消息，则显示一个“ * ”号。默认的超时时间为 4000ms(4s)，用户可以根据自己的网络连接状况设定相应的时间值。

(5) -R：指定 IPv6 路由扩展标头应用来将“回显请求”消息发送到本地主机，使用目标作为中间目标并测试反向路由。

(6) -4：指定 tracert 命令只能将 IPv4 用于本跟踪。

(7) -6：指定 tracert 命令只能将 IPv6 用于本跟踪。

(8) TargetName：指定目标名称，可以是 IP 地址或者目标计算机的名称。

习题

1. 简述 Fluke MicroScanner^2 电缆测试仪的用途。
2. 简述 ping 命令的应用。

实验：使用 Fluke MircoScanner^2

实验目的：

掌握 Fluke MircoScanner^2 的使用方法。

实验内容：

使用 Fluke MircoScanner^2 测试当前网络，实现基本测试任务。

实验步骤：

(1) 测试跳线的连通性。

(2) 测试水平布线系统。

(3) 测试以太网端口。

(4) 测试双绞线长度。

第 9 章 chapter 9

网络协议和资源管理

同人与人之间进行交流的方式是使用相同语言一样，计算机之间实现信息通信也需要相同的“语言”，即网络协议。只有当网络中的两台计算机使用相同的协议时，才可以实现通信。只有正确地配置网络协议，才可以实现计算机之间的资源共享功能。

9.1 网络协议和资源管理规划

网络的基本功能，同时也是最主要的功能就是共享。对于共享资源必须进行严格的管理，如果共享资源管理不善，很有可能会造成无法估量的损失，轻则普通文件丢失，重则机密文件落到“对手”手中。

9.1.1 项目背景

因为在网络中存在多台网络设备、服务器和客户端，这些网络组成部分所使用的网络协议必须相同，否则将无法进行数据传输。在网络中合理地设置共享，可以很大程度上提高网络的使用效率。通常情况下，使用这些共享资源前，需要为所在的计算机配置相应的 IP 地址，在当前网络中因为存在多台服务器和客户端，则需要合理地管理 IP 地址。另外，为了访问共享资源，用户还必须拥有相应的权限。

9.1.2 项目需求

在网络中，数据的传输必须经过所连接的交换机，以及一些所必需的网络设备，当网络中存在大量数据传输时，很有可能是网络中存在不明数据传输，或禁止网络使用的 P2P 软件正在运行，因此，作为管理员需要时刻清楚网络流量中包含哪些数据。因为在网络中不能存在两个相同的 IP 地址，所以必须对 IP 地址资源进行严格的管理。为了节省存储资源，需要所有用户使用相同的文件(例如安装程序等)。“用户”是登录网络的基础，每个网络用户均需拥有一个自己的登录用户账户。另外，由于某些部门中包含多个成员，这些成员的用户权限是相同的。

9.1.3 解决方案

针对于网络协议和资源管理的需求问题，可通过如下方案来解决。

(1) 在网络中安装超级网络嗅探器(Sniffer Pro)，实时监控网络中的流量情况，并可及

时发现异常流量。当发现不明流量时，还可通过网络协议检测工具（Ethereal），对网络中的数据包进行捕获并进行分析。

（2）对于IP地址资源，在划分网络地址时，可使用子网计算工具来完成。在网络正常使用时，为了了解网络中的IP地址使用情况，则可通过IP Address Tracker和IP地址管理工具（IPMaster）来完成。

（3）实现网络资源共享的方法是在网络中部署共享文件夹，将所要共享的文件放置到共享文件夹内，并可针对不同的用户设置不同的权限。

（4）对于用户和组的管理，需要在“Active Directory用户和计算机”窗口中实现。

9.2　网络协议管理

网络分析诊断以网络原理、网络配置和网络运行的知识为基础。从故障现象出发，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源，排除故障，恢复网络正常运行。网络分析诊断应该实现三方面的目的：确定网络的故障点，恢复网络的正常运行；发现网络规划和配置中欠佳之处，改善和优化网络的性能；观察网络的运行状况，及时预测网络通信质量。

9.2.1　超级网络嗅探器——Sniffer Pro

目前，网络分析软件市场占有率最高的是Network Associates公司开发的Sniffer Pro。Sniffer（后文中Sniffer Pro都统称为Sniffer）可以捕获并分析网络数据、分析网络协议等，用于网络故障与性能管理，在网络管理中应用非常广泛。

1. Sniffer简介

Sniffer主要用来分析网络的流量，在众多流量中分析所关心的内容，例如通过使用Sniffer可以判断网络中某台计算机使用网络的具体情况，包括所使用的网络协议、数据流量大小、与哪台计算机相连等信息。另外，当网络发生故障时，可以用嗅探器对问题做出精确的判断，从而提高管理员的工作效率。

Sniffer的功能主要包括如下几方面。

（1）捕获网络流量进行详细分析。

（2）利用专家分析系统诊断问题。

（3）实时监控网络活动情况。

（4）监控单个工作站、会话或者网络中任何一部分的详细的网络利用情况和错误统计。

（5）支持主要的LAN、WAN和网络技术（包括高速与超高速以太网、令牌环、802.11b无线网、SONET传递的数据包、T-1、帧延迟和ATM）。

（6）提供在位和字节水平过滤数据包的能力。

2. Sniffer安装与配置

Sniffer安装位置的选择是使Sniffer发挥作用的关键。通常情况下，Sniffer应该安装在内部网络与外部网络通信的中间位置，例如代理服务器上。也可以安装在局域网内的任意一台计算机上，但此时只能对局域网内部的通信进行分析。

（1）Sniffer的安装

如果网络中使用了代理服务器，那么Sniffer必须安装在代理服务器上，这样Sniffer才

能捕获局域网和 Internet 之间传输的数据。如果使用交换机或路由器方式接入 Internet，可以在网络设备上配置端口镜像，并将网络设备的出口设置为目的端口，然后将安装 Sniffer 的计算机连接到该端口，即可实现对整个网络的监控。

小知识：所谓端口镜像，是指把交换机一个或多个端口(或 VLAN)的数据镜像到一个或多个端口的方法。简单地说，端口镜像就是把交换机一个(数个)端口(源端口)的流量完全复制一份，从另外一个端口(目的端口)发出去。网络管理人员在目的端口通过软件分析源端口的流量，从而找出网络中存在问题的原因。

通常情况下，为了实现对整个网络的监听，应当将网络总出口(如连接至代理服务器、路由器的端口或 VLAN)映射为 Sniffer 计算机所连接的端口。Cisco 的端口镜像叫做 Switched Port Analyzer，简称 SPAN。端口镜像仅适用于以太网交换端口。

Cisco 交换机的 SPAN 端口配置过程如下。

① 进入全局配置模式。

```
Cisco# configure terminal
```

② 为该进程移除任何已经存在的 SPAN 配置。

```
Cisco # no monitor session {session_number | all | local | remote}
```

③ 指定 SPAN 进程和侦听源端口。

```
Cisco (config)# monitor session session_number source {interface interface-id | vlan vlan-id} [,| -]
[both | rx | tx]
```

④ 指定 SPAN 进程与侦听目的端口。

```
Cisco (config)# monitor session session_number destination {interface interface-id [,| -]
```

⑤ 返回特权配置模式。

```
Cisco (config)# end
```

⑥ 校验 SPAN 配置。

```
Cisco # show monitor [session session_number]
Cisco # show running-config
```

⑦ 保存 SPAN 配置。

```
Cisco # copy running-config startup-config
```

例如，若欲将 g1/0/1 端口的所有收发流量全部映射至 g1/0/2 端口，配置过程如下。

```
Cisco (config)# no monitor session 2
Cisco (config)# monitor session 2 source gigabitethernet1/0/1 rx
Cisco (config)# monitor session 2 destination interface gigabitethernet1/0/2
Cisco (config)# end
```

在使用 Sniffer 捕获数据时，由于网络中传输的数据量特别大，如果安装 Sniffer 的计算机内存太小，这些数据会被系统交换到磁盘，从而导致计算机性能下降。如果没有足够的物理内存，很容易造成安装有 Sniffer 的计算机死机或崩溃。因此，网络中捕获的流量越多，安

装 Sniffer 的系统就应该运行得更快、功能更强。因此，建议安装 Sniffer 的系统有一个速度尽可能快的处理器，而且至少应安装 1GB 以上的物理内存。

Sniffer 安装操作比较简单，根据安装向导的提示操作即可，这里就不再赘述。

(2) 配置网络适配器

通常情况下，代理服务器会安装多块网卡，以实现 Internet 共享，而 Sniffer 默认只监控一块网卡上的数据流。因此，在使用 Sniffer 捕获网络数据流前，需要指定所监控的网卡。另外，使用 Sniffer 实例功能，可以实现同时捕获多块网卡，但多个 Sniffer 实例的 Settings 窗口不能同时打开。

① 依次选择"开始"→"所有程序"→Network General→Sniffer Portable→Sniffer Portable 命令，启动 Sniffer 程序。如果当前计算机上安装有多块网卡，会显示图 9-1 所示的 Settings 对话框，需要选择要监视的网卡。

② 为了使 Sniffer 能够监控多个不同的网络，可以设置多个代理。在 Settings 对话框中单击 New 按钮，显示图 9-2 所示的 New Settings 对话框。在 Description 文本框中输入网卡描述信息，在 Network Adapter 下拉列表框中选择要使用的网卡。

③ 单击 OK 按钮，保存设置即可。

④ 配置完成后，单击"确定"按钮，显示图 9-3 所示的 Sniffer Portable Field Service 窗口。依次选择 File→Settings 命令，选择不同的网卡，即可监控不同的网络。

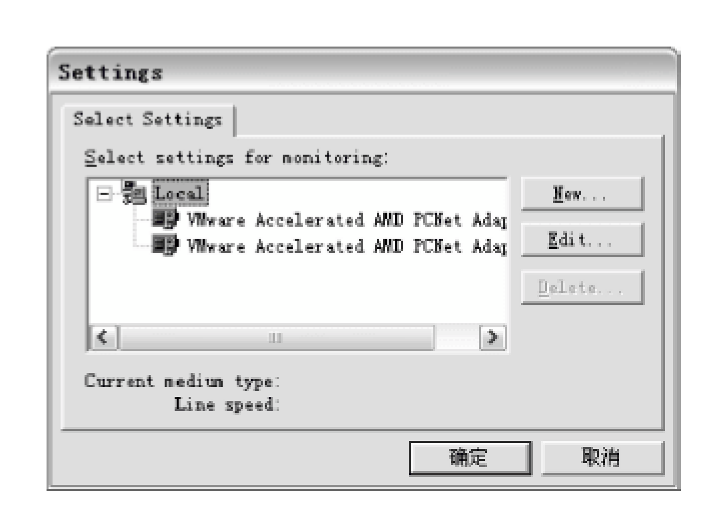


图 9-1 设置网络适配器

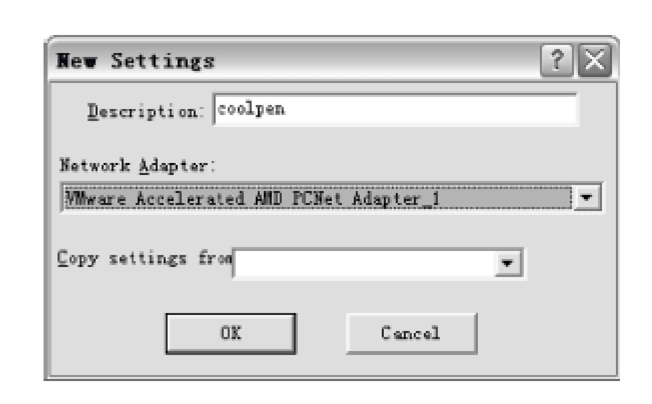


图 9-2 New Settings 对话框

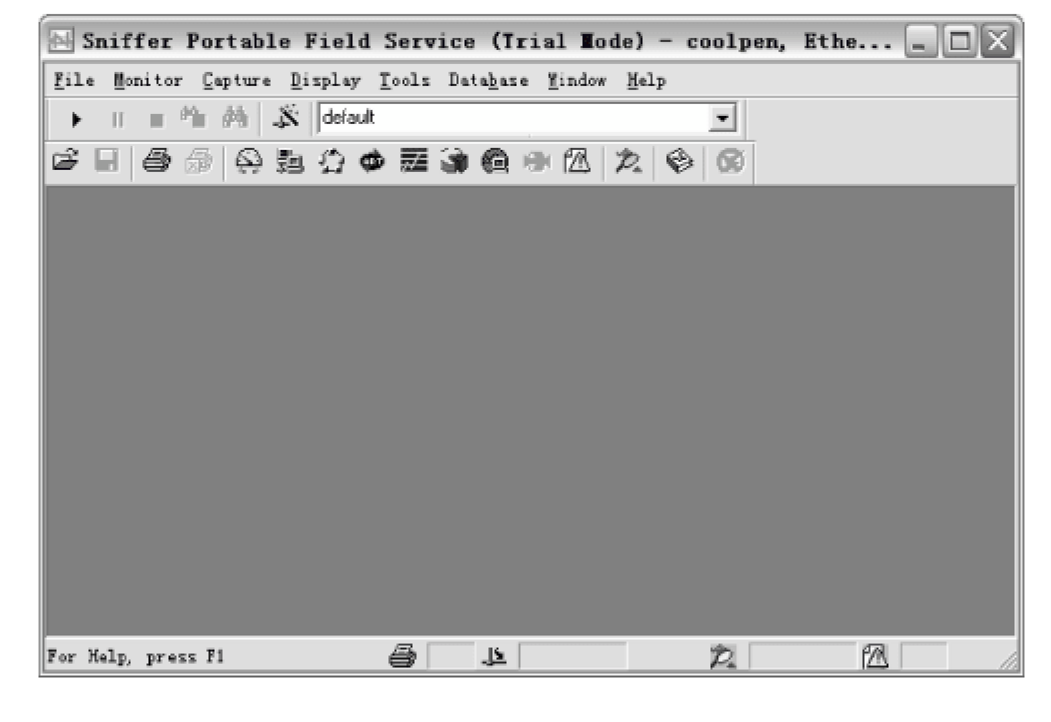


图 9-3 Sniffer 主窗口

3. Sniffer 的监控模式

Sniffer 的监控功能可以查看当前网络中的数据传输情况。Sniffer 具有 7 大监控功能，即 Dashboard（仪表）、Host Table（主机列表）、Matrix（矩阵）、ART（Application Response Time，应用响应时间）、Protocol Distribution（协议分类）、History Samples（历史采样）和 Global Statistics（全局统计）。这些功能可以实时显示当前网络中传输的数据，便于网络管理员及时发现故障并解决。

(1) Dashboard（仪表）

Sniffer 的仪表盘使用图形化界面，可以直观地观测到网络的利用情况。

在 Sniffer 窗口中，依次选择 Monitor→Dashboard 命令，或单击工具栏上的仪表盘按钮，显示图 9-4 所示的仪表盘窗口，以后每次启动 Sniffer 时都会自动打开该仪表盘。这里共有 3 个仪表盘，分别为 Utilization%、Packets/s 和 Errors/s，分别用来显示网络利用率、传输的数据和错误统计。其中，表盘的红色区域表示警戒值，下方的两个数字分别表示当前和最大的利用率。

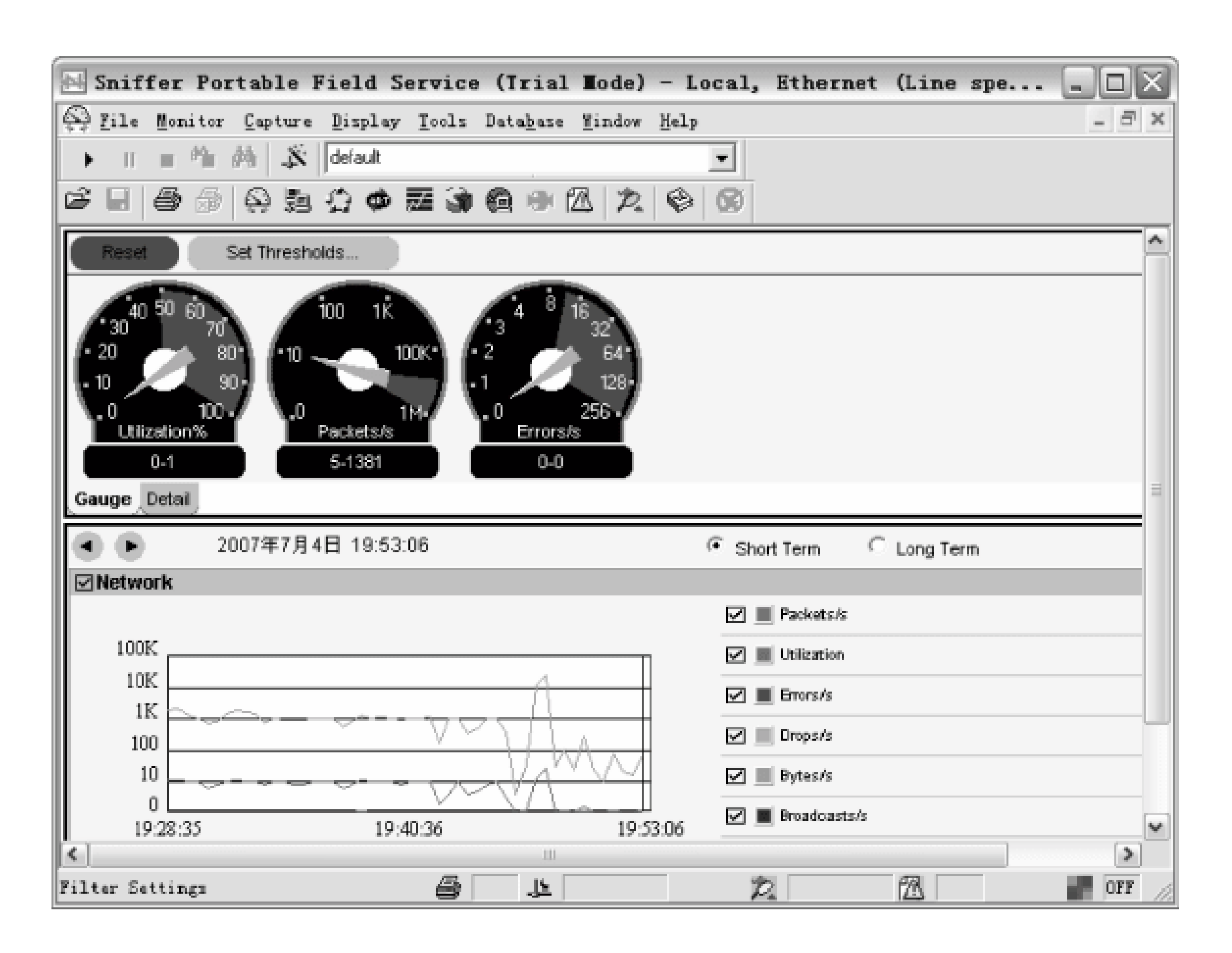


图 9-4 Sniffer 主界面

通过这 3 个仪表盘，管理员可以很容易地看到从捕获开始，有多少数据包经过网络、多少帧被过滤，以及遗失了多少帧。还可以看到网络的利用率、数据包数目和广播数，如果发现网络在每天的特定时间都会收到大量的组播数据包，这说明网络可能出现了问题，需及时分析哪个应用程序在发送组播数据包。

各个表盘的作用分别如下。

① Utilization%(利用率百分比)：使用传输与端口能处理的最大带宽的比值来表示网络占用带宽的百分比。由于网络数据流通常都是突发的，一个几秒钟内爆发的数据流和能长期保持活性数据流的重要性是不同的，因此，表示网络利用率的理想方法要因网络不同而改变，而且很大程度上要取决于网络的拓扑结构。在以太网端口，利用率为 40%，效率可能已经很高了，但是在全双工可转换端口，80%的利用率才是高效的。

② Packets/s(每秒传输的数据包)：显示网络中当前数据包的传输速率，例如，如果网络利用率很高，而数据包传输速率相对较低，则说明网络上的帧比较大；如果网络利用率很高，数据包传输速率也很高，说明帧比较小。通过查看规模分布的统计结果，可以更详细地了解帧的大小。

③ Errors/s(每秒产生的错误)：显示当前网络中的出错率，但并非所有的错误都产生故障，例如，以太网中经常会发生冲突，并不一定会对网络造成影响，但过多的冲突就会带来问题。

提示：每个仪表盘下方都会显示两个数值，前一个数值表示当前值，后一个数值表示最大值。

如果想查看详细的传输数据，可单击仪表盘下方 Detail(详细)按钮，显示图 9-5 所示的表格，以数值形式显示网络的使用信息。

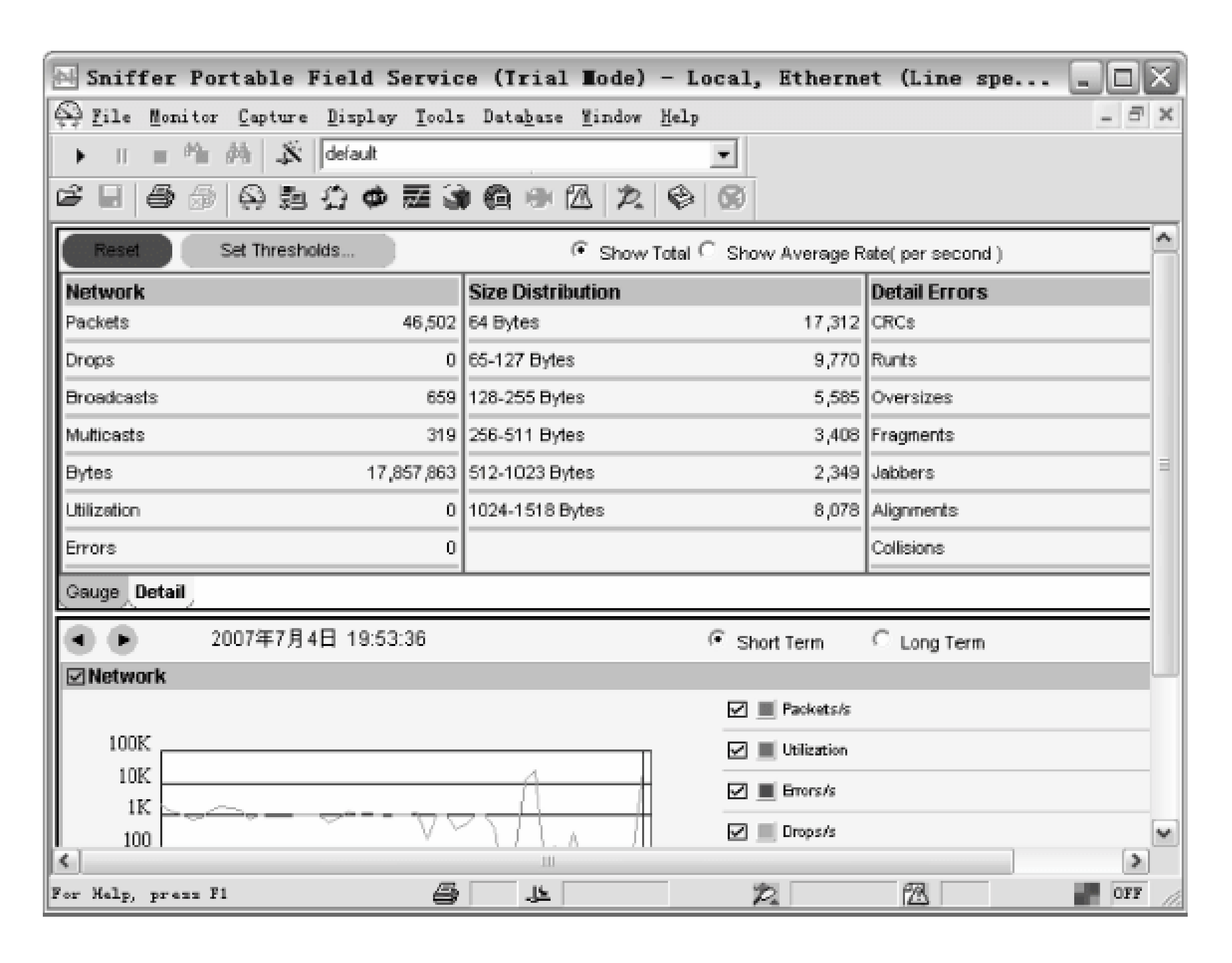


图 9-5　表格形式

其中，Network 表格中显示了当前网络的使用情况。

① Packets：网络中传输的数据包总数。

② Drops：网络中遗失的数据包数量（在网络活动高峰期经常会遗失数据包）。

③ Broadcasts：网络中广播帧的数量。子网或 VLAN 上所有的组件都必须处理所有的广播数据包，过多的广播会使网络上所有系统的性能整体下降。

④ Multicasts：网络中组播帧的数量。

⑤ Bytes：数据包的总字节数。

⑥ Utilization：当前网络的利用率。

⑦ Errors：网络中存在的错误的总数。

在 Size Distribution 表格中列出了网络中数据包（包括 4 字节的 CRC）的分布状态，包括 64Bytes、65～127Bytes、128～255Bytes 等各种不同字节的数据包总数。Detail Errors 表格中列出了错误出现率，即 Errors/s 表盘中显示的错误的详细情况。

Sniffer 的很多网络分析结果都可以设定阈值，若超出阈值，报警记录就会生成一条信息，并在仪表盘上以红色来标记阈值的警告值。网络管理员可根据警告信息，通过对超过阈值的次数和超出阈值的频率进行分析，从而判断网络的健康状况。

单击仪表盘上的 Set Thresholds（设定阈值）按钮，显示图 9-6 所示的 Dashboard Properties 对话框，根据网络状况配置仪表阈值即可，以保证仪表能准确地显示网络情况。

（2）Host Table（主机列表）

Sniffer 的主机列表功能是以列表形式显示当前网络上计算机的流量信息。

依次选择 Monitor→Host Table 命令，显示图 9-7 所示的窗口，查看当前所捕获的网络上的各个主机的流量信息。

① Hw Addr（硬件地址）：以 MAC 地址形式显示计算机。

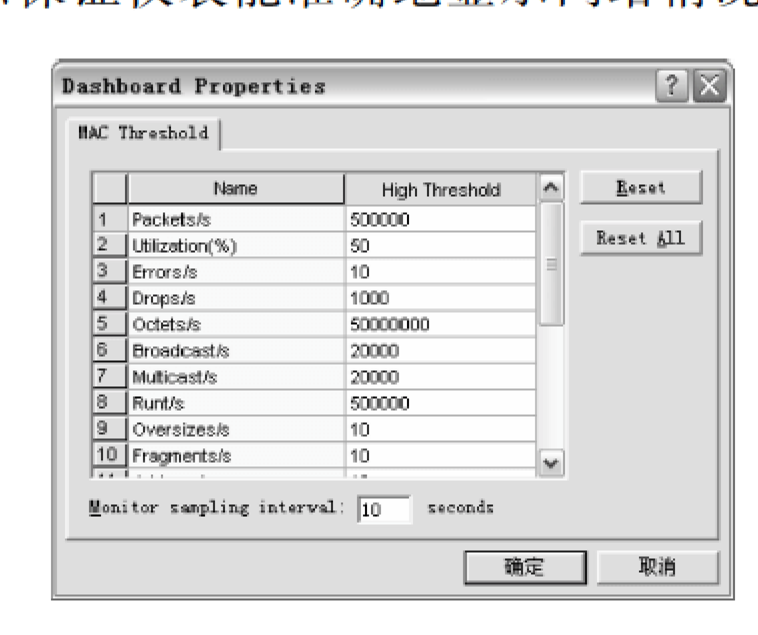


图 9-6　Dashboard Properties 对话框

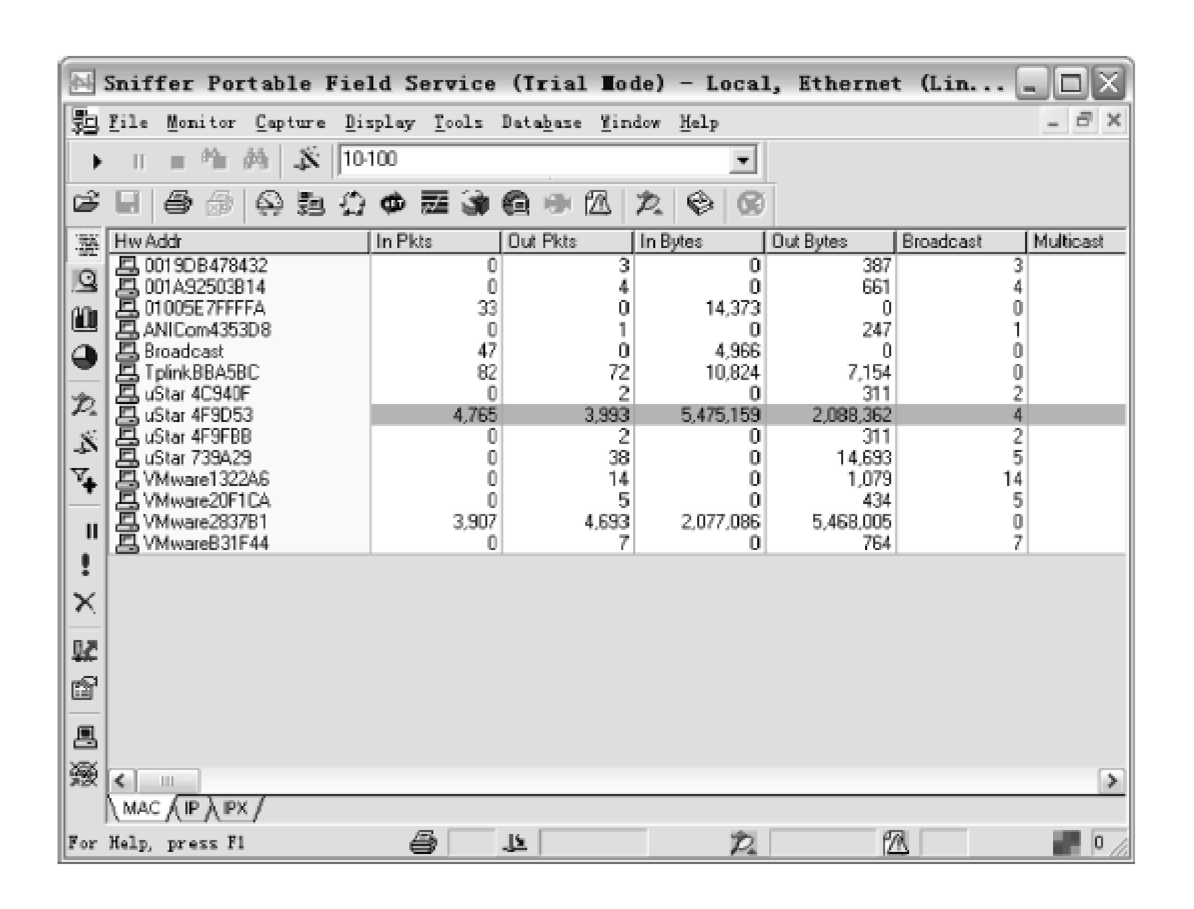


图 9-7 主机列表

② In Pkts(传入数据包):网络上发送到此主机的数据包。

③ Out Pkts(传出数据包):本地主机发送到网络上的数据包。

④ In Bytes(传入字节数):网络上发送到此主机的字节数。

⑤ Out Bytes(传出字节数):本地主机发送到网络上的字节数。

在查看网络主机信息时,默认以 MAC 地址形式显示网络中的计算机。如果计算机处于局域网中,可以清楚地显示计算机的 MAC 地址。如果计算机处于 Internet 中,则不能获得计算机的 MAC 地址,此时会以 IP 地址形式显示。选择窗口下方的 IP 选项卡,如图 9-8 所示,即可显示计算机的 IP 地址。

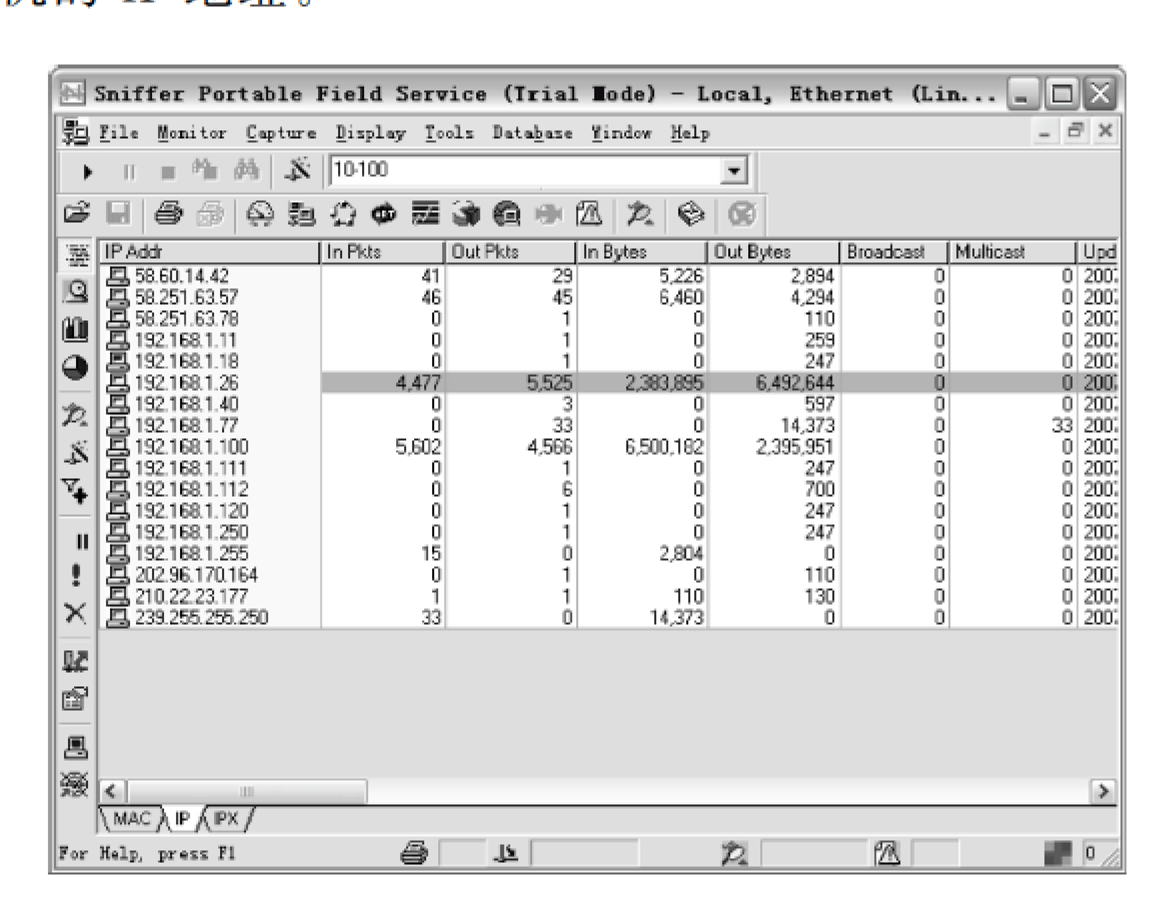


图 9-8 以 IP 地址形式显示

提示:通过主机列表功能,可以查看某台计算机所传输的数据量。如果发现某台计算机在某个时间段内发送或接收了大量数据,例如某用户一天内就传输了数 GB 的数据,则说明该用户很可能在使用 BT、PPLive 等 P2P 软件。

(3) Matrix(矩阵)

Matrix 是 Sniffer 中最常用的功能之一,以矩阵方式列出当前网络中的连接情况。管理员通过它清楚地掌握某计算机正在与哪些地址进行连接,并可查看因蠕虫、BT 软件等造

成的网络异常情况。

在 Sniffer 主窗口中，依次选择 Monitor→Matrix 命令，显示图 9-9 所示的窗口，显示了当前所捕获的网络中各计算机的连接情况。选择窗口下方的 IP 选项卡，可以以 IP 地址方式显示各主机。

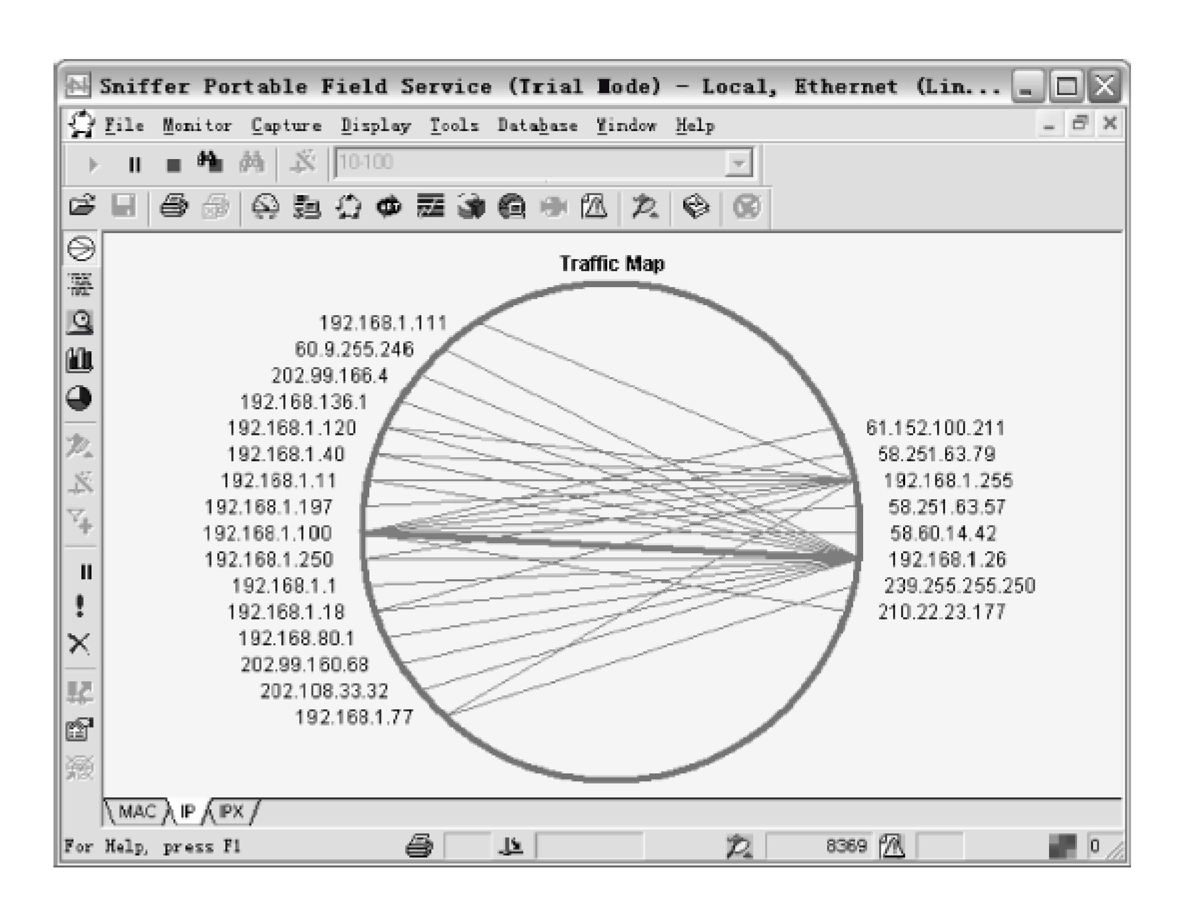


图 9-9　矩阵窗口

在窗口空白处右击，从快捷菜单中选择 Zoom 命令，在子菜单中选择 100%、200%、300%等命令，可以放大显示比例，以解决因为连接过多或连接太密集而无法查看具体连接情况的问题。

如果要详细查看某台主机的连接情况，可以在该窗口中只显示该主机的连接。右击要查看的主机 IP 地址，在快捷菜单中选择 Show Select Nodes 命令，显示如图 9-10 所示，此时可以清楚地看到该计算机正在与哪些地址连接。如果将鼠标指针放在连线上，还会显示出该主机所传输的数据大小。右击窗口并选择快捷菜单中的 Show All 命令，即可返回查看所有主机的连接情况。

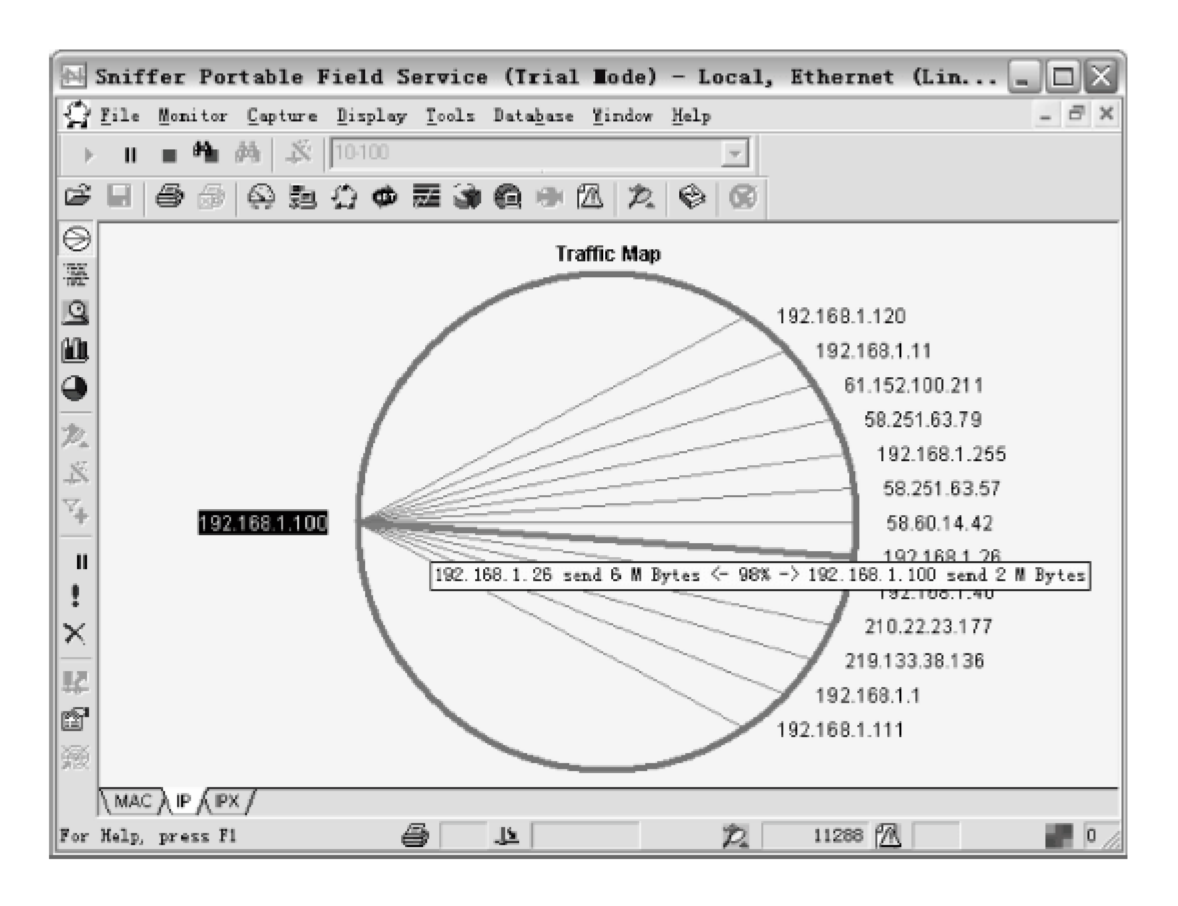


图 9-10　显示单个主机的连接情况

小知识：通过 Matrix 功能，管理员可以发现网络中使用 BT 等 P2P 软件或中了蠕虫病毒的用户。如果某个用户的并发连接数特别多，并且不断地向其他计算机发送数据，这就说

明该计算机很可能中了蠕虫等病毒。此时，网络管理员应及时封掉该计算机所连接的交换机端口，并对该计算机查杀病毒。

（4）Application Response Time（应用响应时间）

Sniffer 的 Application Response Time 功能主要用来显示网络中 Web 网站的连接情况，可以看到局域网中有哪些计算机正在上网，浏览的是哪些网站等。

在 Sniffer 主窗口中，依次选择 Monitor→Application Response Time 命令，显示图 9-11 所示的 Application Response Time 对话框。其列表框中显示了局域网内的通信及数据传输大小，并且显示了本地计算机与 Web 网站的 IP 地址。

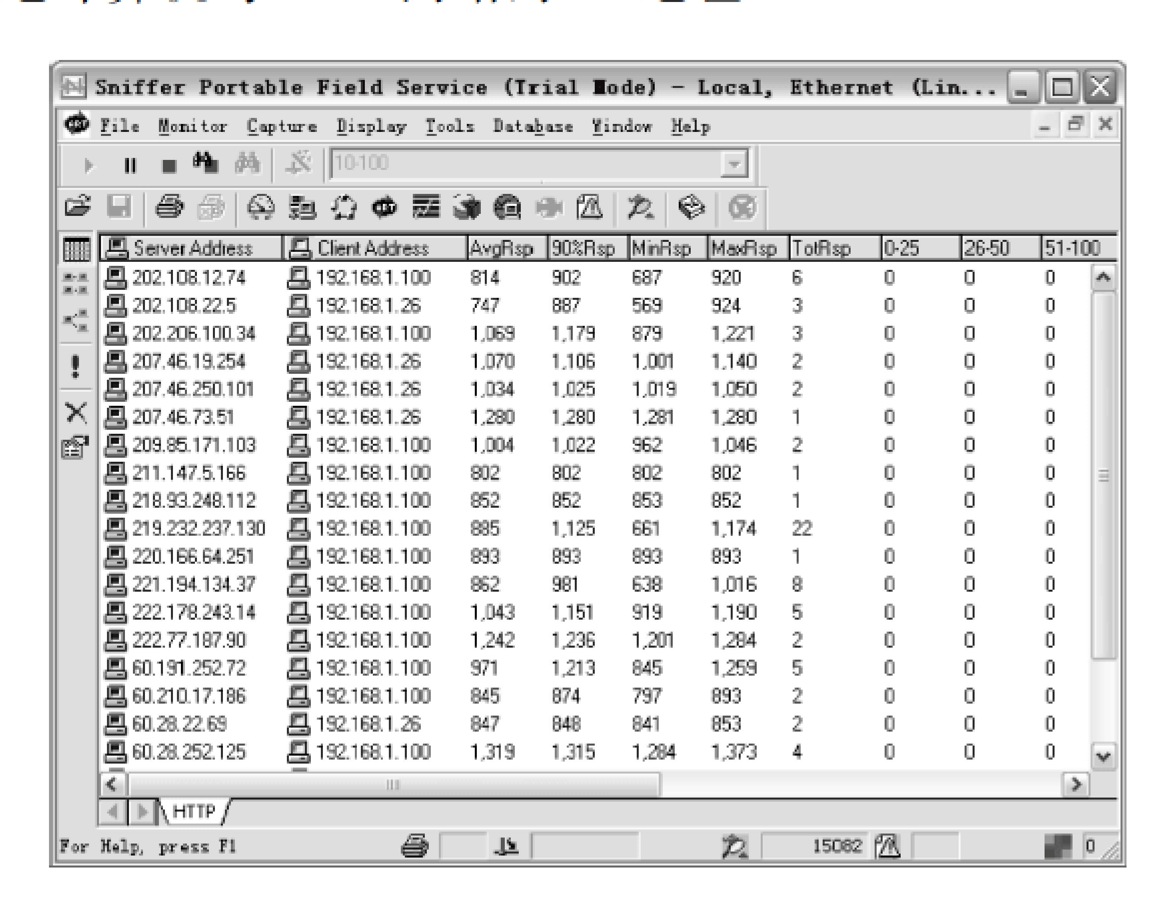


图 9-11 应用程序响应时间

通过单击左侧工具栏中的图标，可以以柱形图方式显示网络中计算机的数据传输情况。不同顺序的图形柱代表右侧列表中的相应的连接，并以柱形的长短显示传输量的大小，如图 9-12 所示。

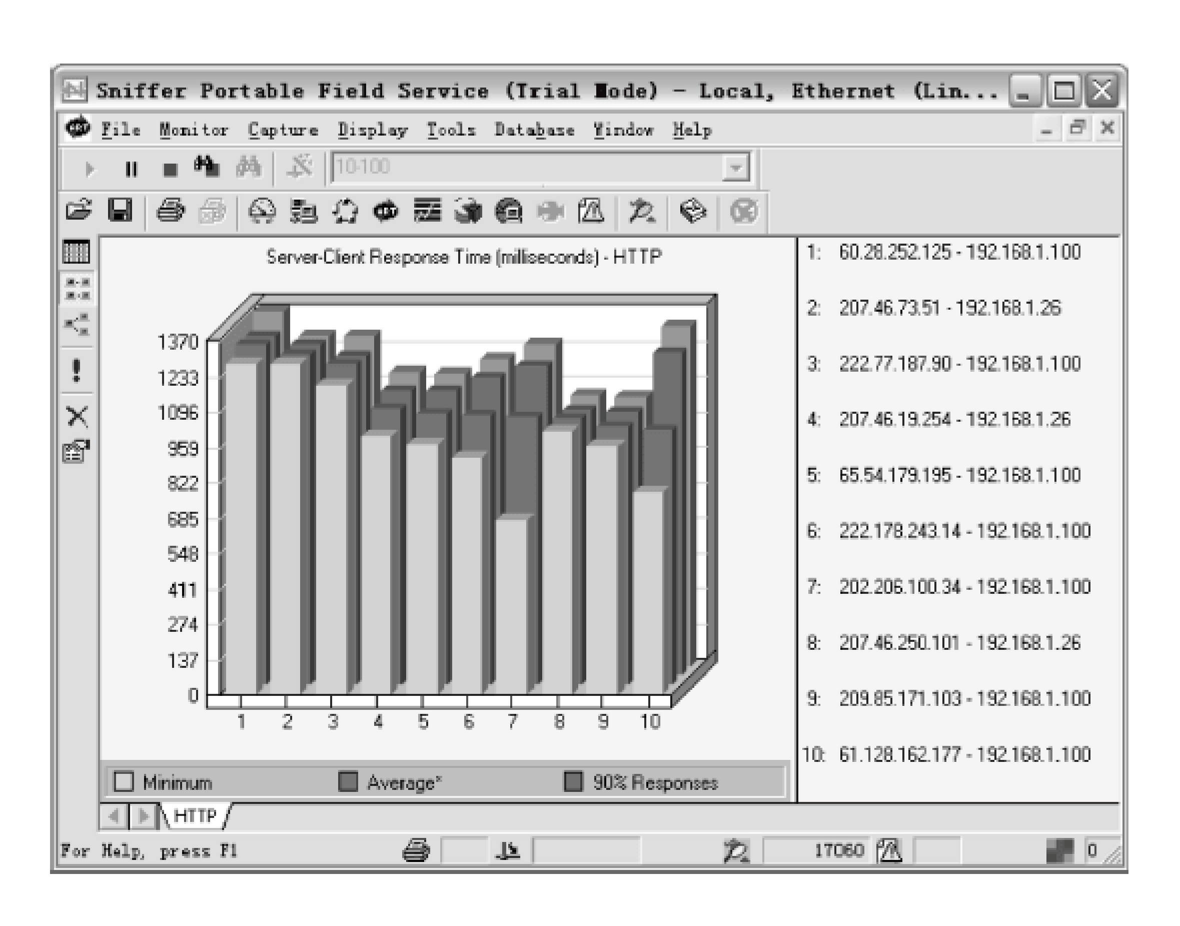


图 9-12 服务器-客户响应时间柱形图

（5）History Samples（历史采样）

Sniffer 的历史采样功能记录了捕获过程中各个时间段的网络利用情况。在 Sniffer 主

窗口中，依次选择 Monitor→History Samples 命令，显示图 9-13 所示的窗口，包括了多种记录。

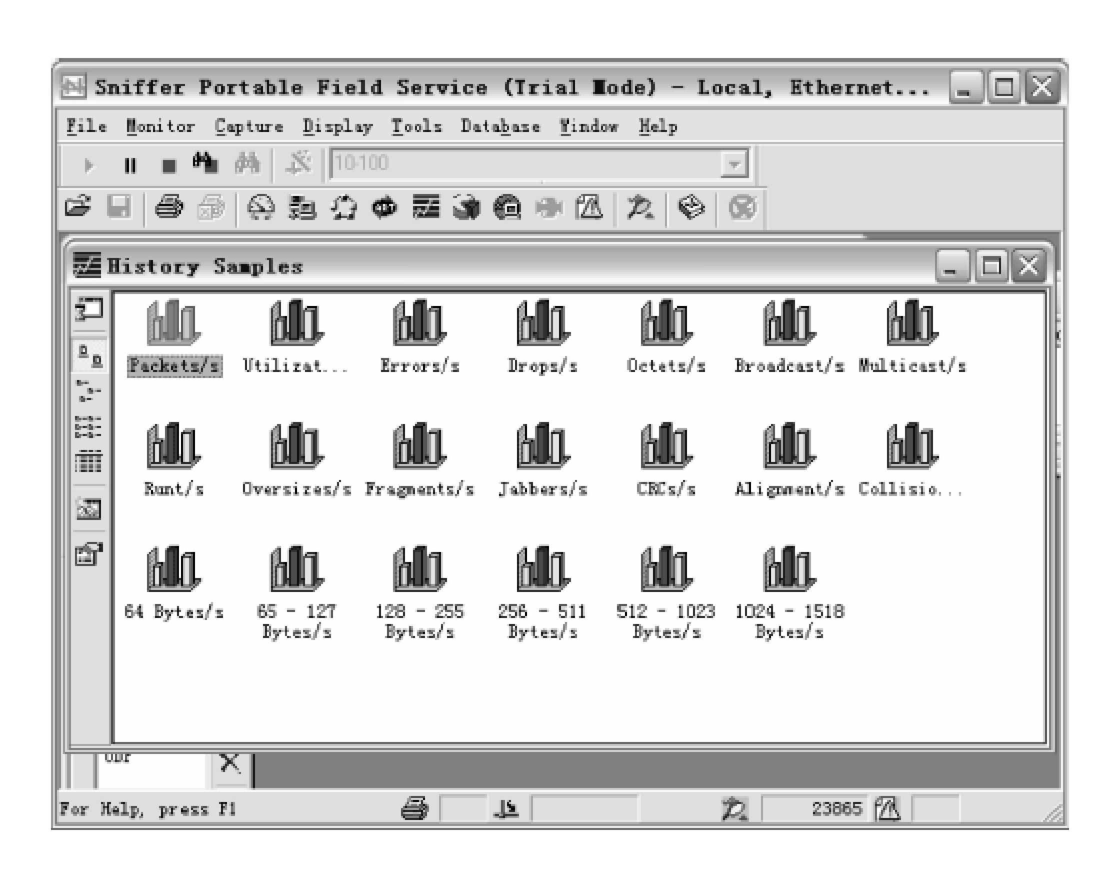


图 9-13　History Samples 窗口

要查看一个网络中每秒发送的数据包数，双击 Packets/s 图标，显示图 9-14 所示 Packets/s 窗口，Sniffer 便开始记录每秒所发送的数据包数量，并且每隔 15 秒钟便记录一次，以柱形方式显示。

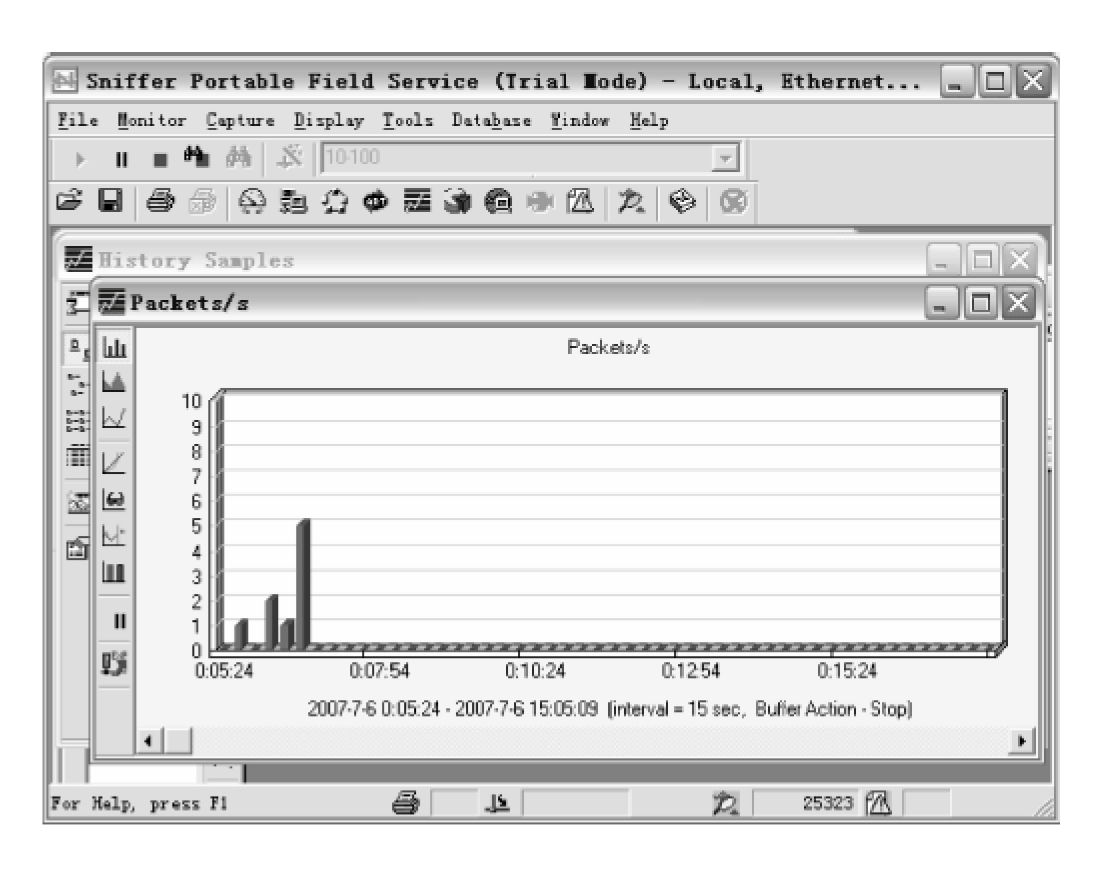


图 9-14　Packets/s 窗口

经过一段时间的记录后，便可以将记录结果保存起来，便于管理员分析各个时间段的数据流量。依次选择 File→Save 命令保存即可。

（6）Protocol Distribution（协议分类）

在 Sniffer 主窗口中，依次选择 Monitor→Protocol Distribution 命令，显示图 9-15 所示的窗口，以不同颜色的柱形显示网络中不同协议的使用情况。

通过单击左侧工具栏上饼形、表格形图标，还可以分别以饼形、表格等方式显示。图 9-16 所示为以表格方式显示。

（7）Global Statistics（全局统计）

Sniffer 的 Global Statistics 功能用来显示不同大小数据包的使用情况。

在 Sniffer 主窗口中，依次选择 Monitor→Global Statistics 命令，显示图 9-17 所示的窗

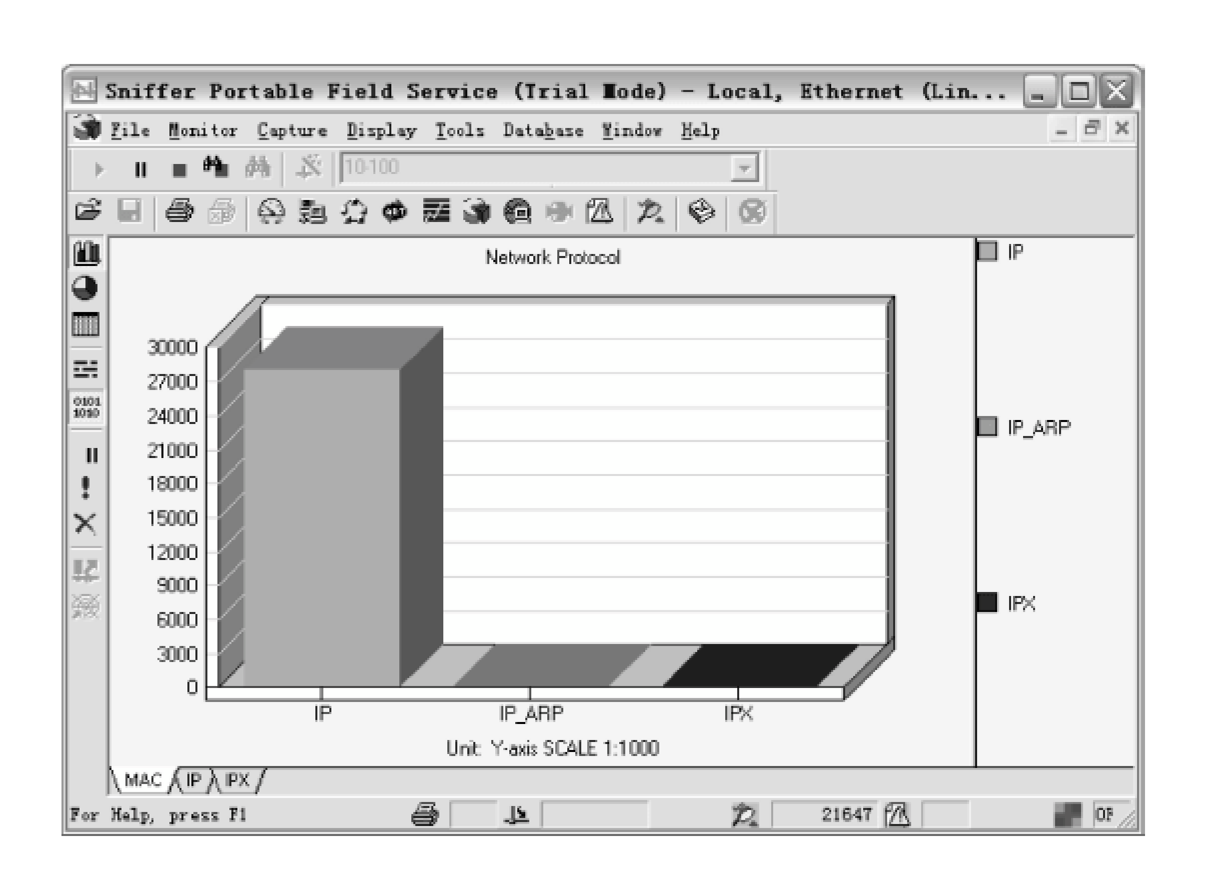


图 9-15　协议使用情况

口，默认以柱形方式显示不同大小数据包的使用情况。也可以单击左侧工具栏中的柱形图标，以柱形方式显示。

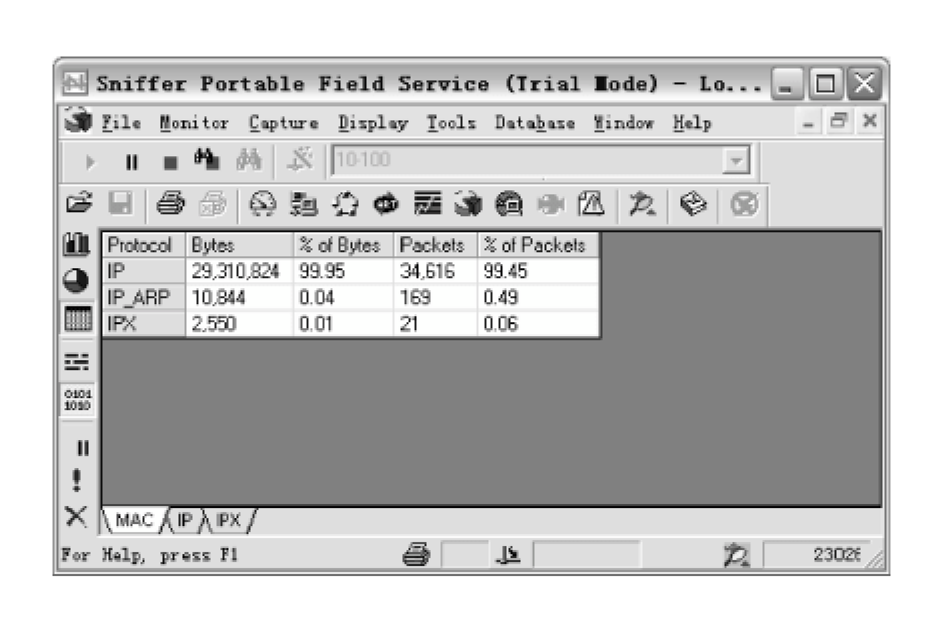


图 9-16　以表格方式显示

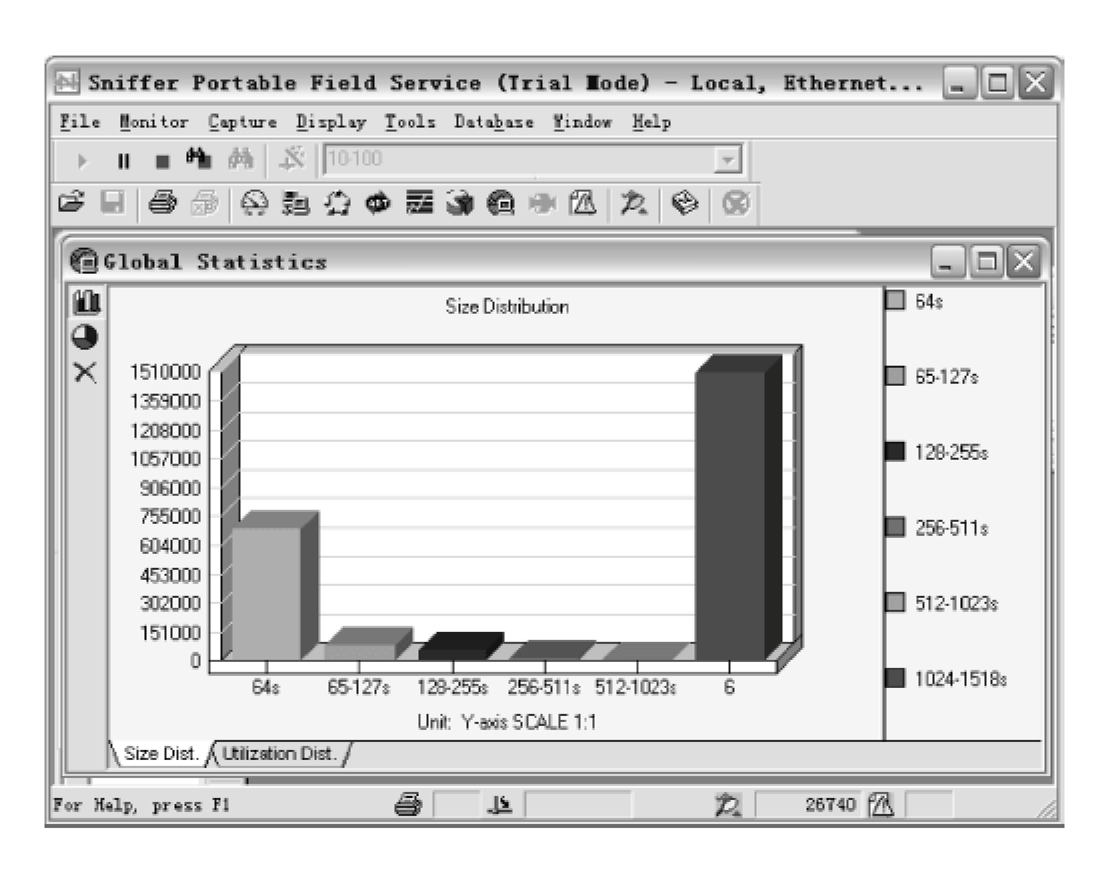


图 9-17　Global Statistics 对话框

4. 创建过滤器

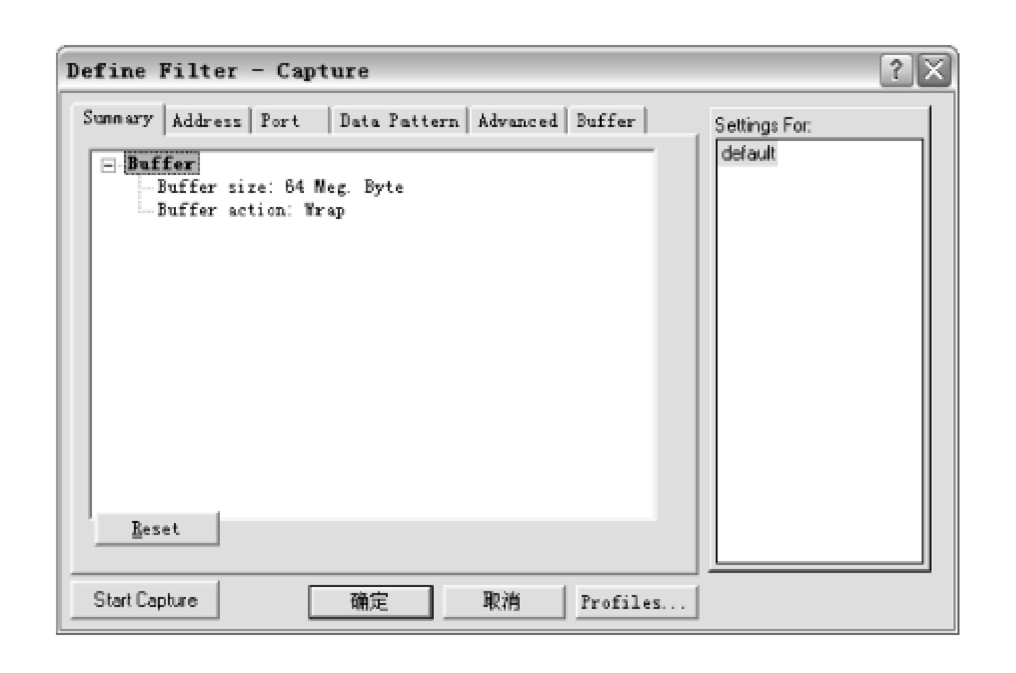
默认情况下，Sniffer 会监控网络中所有传输的数据包，但在分析网络协议、查找网络故障时，有许多数据包并不是管理员所关心的。通过定义过滤器，管理员可以设定捕获条件，Sniffer 只接收与问题或事件相关的数据，从而便于进行数据分析。Sniffer 提供了捕获数据包前的过滤规则的定义功能，过滤规则包括 2、3 层地址的定义和几百种协议的定义。

(1) 过滤 IP 地址

这里创建一个过滤器，使 Sniffer 只捕获 IP 地址段为 192.168.1.10～192.168.1.100 范围内传输的数据。

① 在 Sniffer 主窗口中，设置过滤方式，依次选择 Capture→Define Filer 命令，显示图 9-18 所示的 Define Filter - Capture 对话框。在 Settings For 列表框中显示过滤器名，默认只有 default 过滤器，该过滤器对所有经过网卡的数据全部捕获。

② 单击 Profiles 按钮，显示图 9-19 所示的 Capture Profiles 对话框。



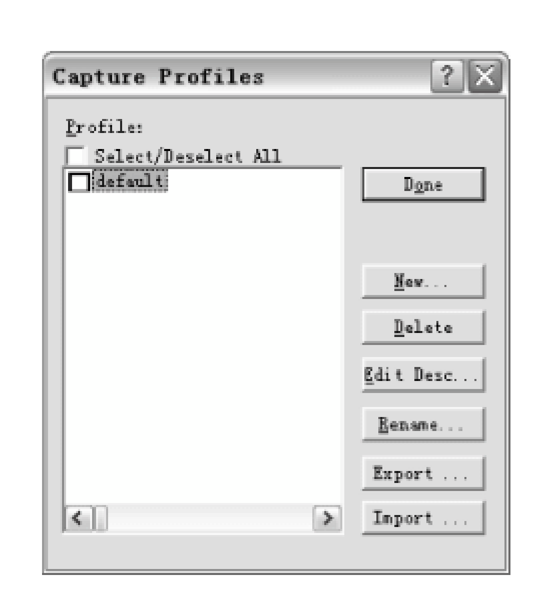



图 9-18 Define Filter - Capture 对话框　　图 9-19 Capture Profiles 对话框

③ 单击 New 按钮，显示图 9-20 所示的 New Capture Profile 对话框，在 New Profile Name 文本框中输入新过滤器的名称，如 10-100。

④ 单击 OK 按钮返回 Capture Profiles 对话框，一个新的过滤器创建完成，并添加到 Profiles 列表中，单击 Done 按钮返回 Define Filter - Capture 对话框，新过滤器将显示在 Settings For 列表中。

⑤ 在 Settings For 列表框中，选择过滤器 10-100，选择 Address 选项卡，在 Station 列表中用来设定要监视的 IP 地址范围。分别在 Station 1 和 Station 2 中输入 IP 地址 192.168.1.10 和 192.168.1.100，如图 9-21 所示。

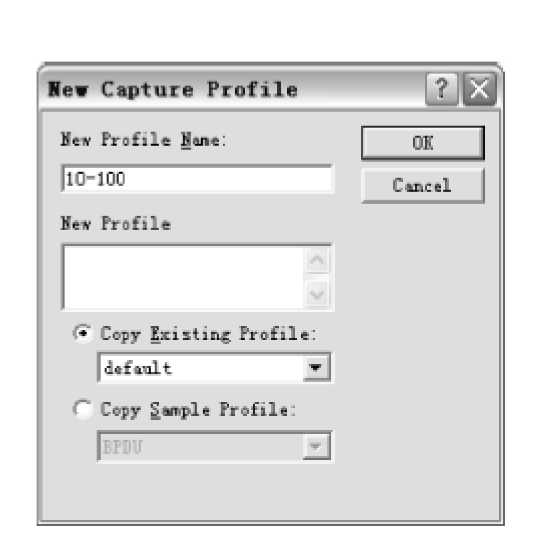


图 9-20 New Capture Profile 对话框

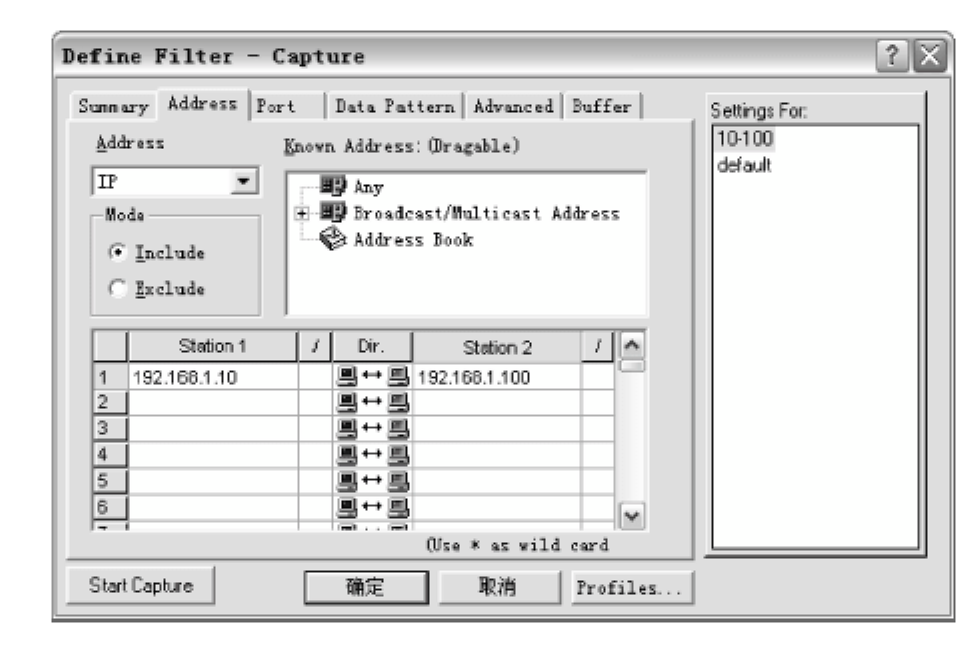


图 9-21 Address 选项卡

⑥ 单击“确定”按钮，过滤器创建完成。

在网络管理过程中，应设定多个过滤器，根据不同的监控用途进行选择。在 Sniffer 窗口中，依次选择 Capture→Select Filter 命令，显示 Select Filter 对话框，在左侧列表中即可选择要使用的过滤器，并可看到过滤器设定的条件，如图 9-22 所示。单击“确定”按钮，应用所选择的过滤器，Sniffer 会根据过滤器所设置的条件来捕获网络中特定的数据。

(2) 过滤端口

Sniffer 4.8/4.9 中增加了端口过滤功能，可以让 Sniffer 只捕获特定端口内传输的数据，可以是固定的一个或几个端口，也可以是一个端口范围。这里创建一个过滤器，只捕获 80 和 445 端口所传输的数据，来监控网络中访问 Internet 网页和网络共享的数据。

① 首先，按照上述操作先创建一个过滤器，如 80-445。在 Define Filter - Capture 对话框中，选择 Port 选项卡，在 Port 1 的 1 和 2 文本框中分别输入 80、445，Port 2 中为 Any 即

可，如图 9-23 所示。

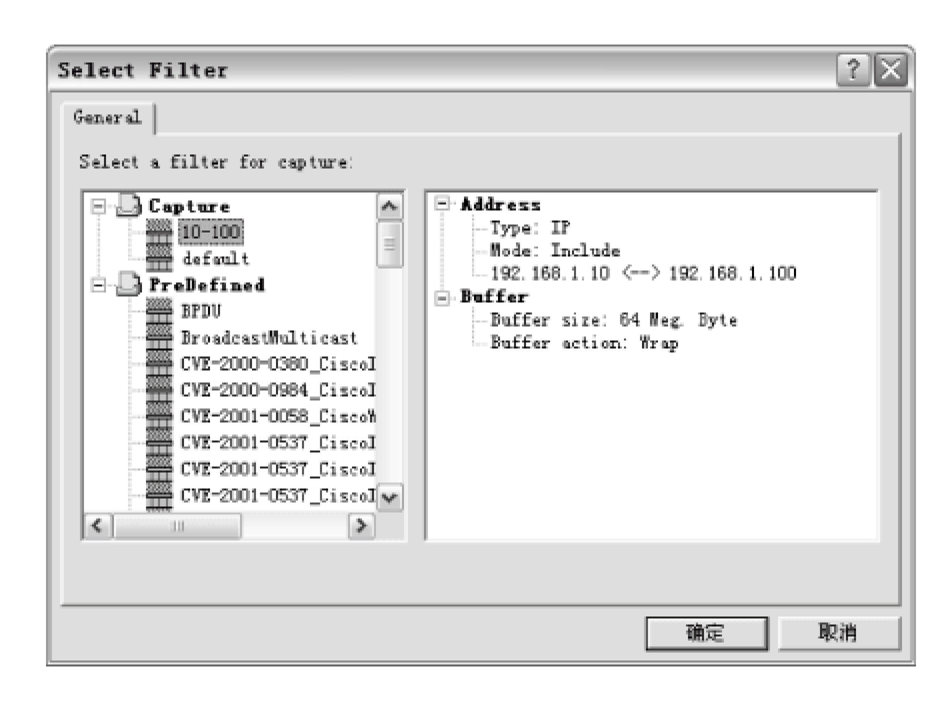


图 9-22 Select Filter 对话框

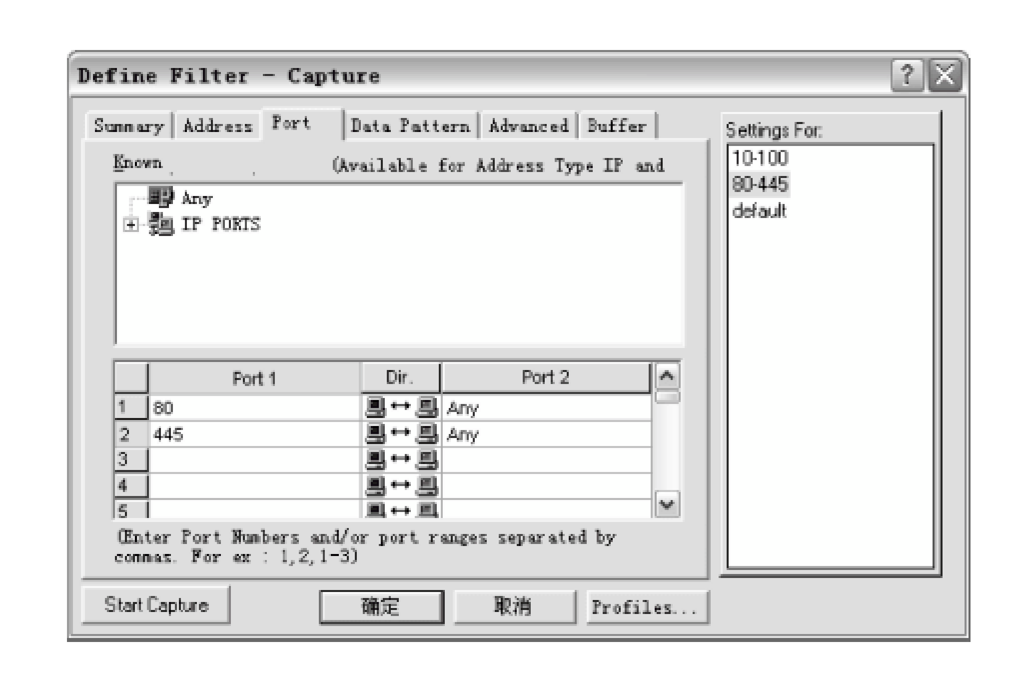


图 9-23 Port 选项卡

② 单击“确定”按钮，只捕获 80 和 445 端口数据的过滤器创建成功。在选择使用该过滤器监控网络时，Sniffer 就会只捕获网络中通过端口 80 和 445 的数据，从而了解网络资源的占用情况。

(3) 过滤网络协议

虽然 Sniffer 可以通过 IP 地址、端口等形式捕获数据，但如果客户端更改了 IP 地址，或一些软件使用随机端口，如 BT、PPLive 等软件，每次都使用不同的端口，那么 Sniffer 将很难捕获到相应的数据。此时，可以根据网络协议进行捕获，Sniffer 支持网络中大部分的网络协议，无论客户端怎样更改，软件所使用的协议是不会变的，通过监控协议，可以使各种软件无所遁形。

这里创建一个过滤器，只捕获网络中使用 FTP 协议传输的数据，来查看有多少人在通过 FTP 下载文件。

① 创建一个新过滤器，例如 FTP。

② 选择 FTP 过滤器，选择 Advanced 选项卡，依次展开 Available→Protocols→IP→TCP 目录，选中 FTP 复选框，使该过滤器只捕获使用 FTP 协议传输的数据。

③ 单击“确定”按钮保存，即可使 Sniffer 使用该过滤器只捕获使用 FTP 协议传输的数据。

(4) 设置缓冲器

缓冲器用来临时保存 Sniffer 捕获的数据，它占用的是计算机的内存。当缓冲器已满后，Sniffer 就会自动停止捕获，但缓冲器中的内容不会自动保存，当重新捕获或关闭 Sniffer 时，缓冲器会自动清空。Sniffer 4.9 的缓冲器大小默认为 64MB，比以前版本大了许多。网络管理员可以创建一个过滤器，自定义缓冲器的大小，并可设置将缓冲器中的数据保存到文件中，以备日后进行分析。

这里创建一个捕获网络中使用 HTTP 协议数据的过滤器，设置缓冲区大小为 40MB，缓冲器中的数据保存到 E:\sniffer 文件夹下。

① 创建一个过滤器，如 new buffer，选择 Advanced 选项卡，依次选择 IP→TCP→HTTP 选项。

② 选择图 9-24 所示的 Buffer 选项卡，在 Buffer size 下拉列表框中选择 40MB 选项，在 Capture buffer 选项区域中，选中 Save to file 复选框，在 Director 文本框中输入地址 E:\

sniffer\，或单击“浏览”按钮选择保存目录即可，在 Filename 文本框中设置保存的文件名。

③ 单击“确定”按钮，新过滤器创建完成。当 Sniffer 使用该过滤器捕获时，即可将捕获的数据保存到文件中。

（5）过滤器的使用

在 Sniffer 中，新创建的过滤器会被设置为默认过滤器，当单击 Start 按钮时就会自动使用新过滤器捕获数据。如果要使用其他过滤器，则需要重新选择。

① 依次选择 Capture→Select Filter 命令，显示图 9-25 所示的 Select Filter 对话框，在左侧的列表框中显示了所有的过滤器。其中，Capture 列表中显示的是用户自定义的过滤器，而 PreDefined 列表中则是 Sniffer 内置的过滤器。当选择一个过滤器后，在右侧窗格中会显示该过滤器定义的详细信息。

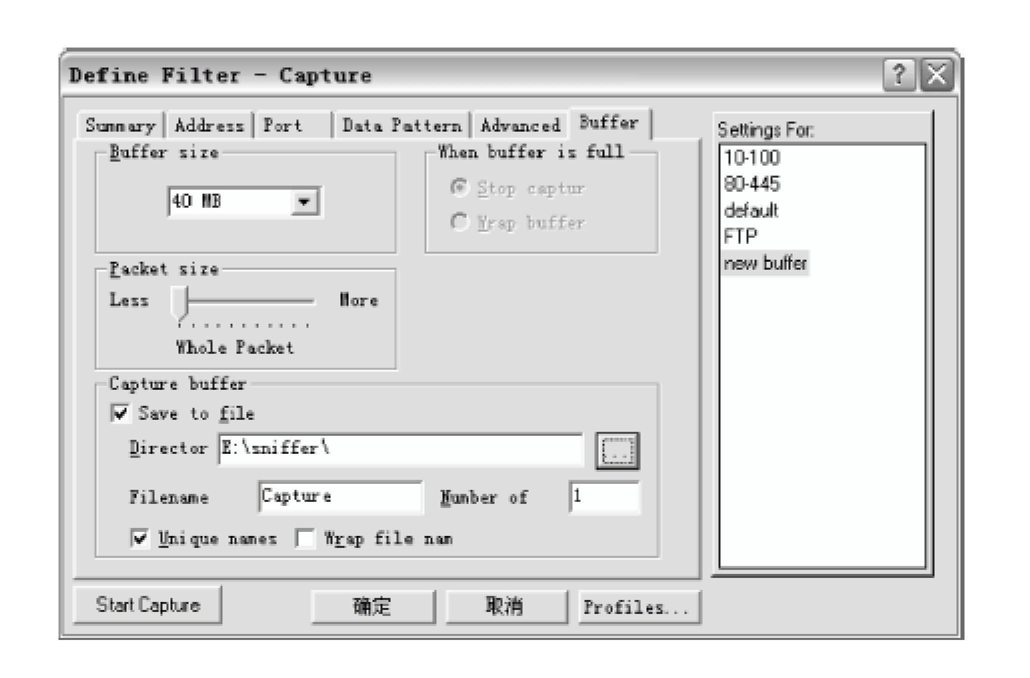



图 9-24　Buffer 选项卡

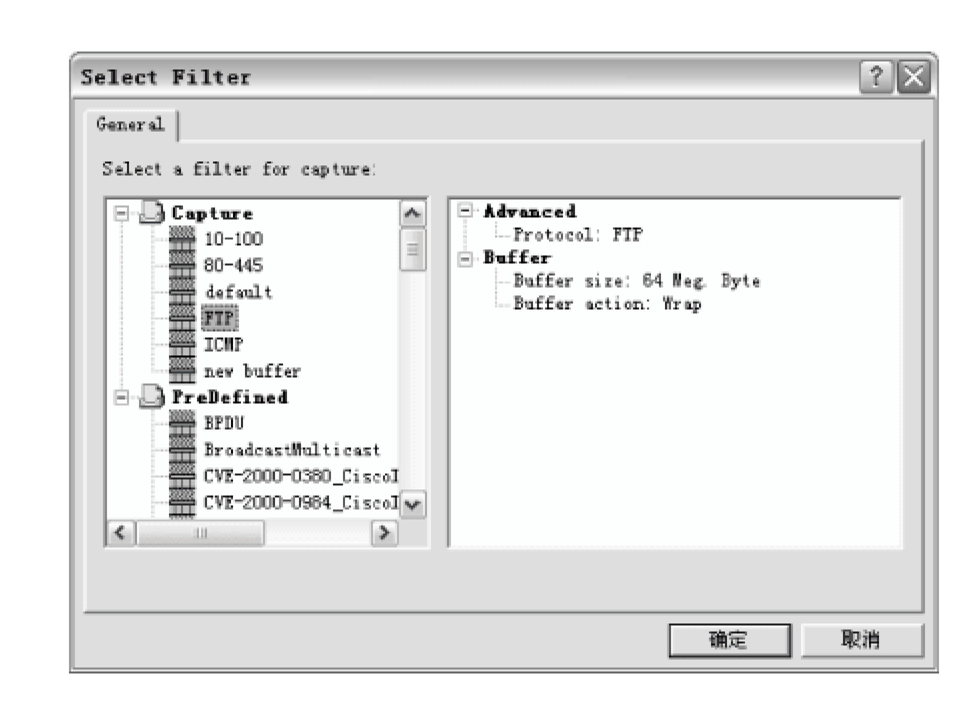


图 9-25　Select Filter 对话框

② 单击“确定”按钮即可应用。

③ 单击 Start 按钮，即可根据所选择的过滤器中定义的条件捕获网络中的数据。

另外，Sniffer 中所有的过滤器都会显示在工具栏上的下拉列表框中，在该下拉列表框中单击要使用的过滤器，然后单击 Start 按钮，即可根据选择的过滤器捕获数据。

5．Sniffer 的使用

通常情况下，Sniffer 根据所设置的过滤器捕获数据，管理员再对这些数据进行分析，并从中发现网络中所存在的问题。如果捕获到的数据比较重要，还可以将这些数据进行保存，从而可以在日后进行详细的分析。

（1）捕获数据

通过 Sniffer 进行网络和协议分析，需要先捕获网络中的数据。默认状态下，由于 Sniffer 没有进行过滤设置，会捕获网络中所有的数据。

① 单击工具栏上的 ▶ 按钮，或依次选择 Capture→Start 命令，显示 Expert 窗口，Sniffer 开始捕获网络中的数据，并显示所捕获到的数据的概要信息，如图 9-26 所示。

② 如果要查看当前捕获的各种数据，单击对话框左侧的 Service、Connection 等选项，在右侧即可显示相应数据的概要信息。选择窗口左侧的 Objects 选项卡，可显示出当前所监视对象的详细信息，如图 9-27 所示。

③ 当 Sniffer 捕获了一定的数据，就可以停止捕获并进行分析。单击工具栏上的■按钮，或依次选择 Capture→Stop 命令，即可停止捕获。此时，管理员可以查看并分析所捕获的数据，从而了解网络的使用状况。

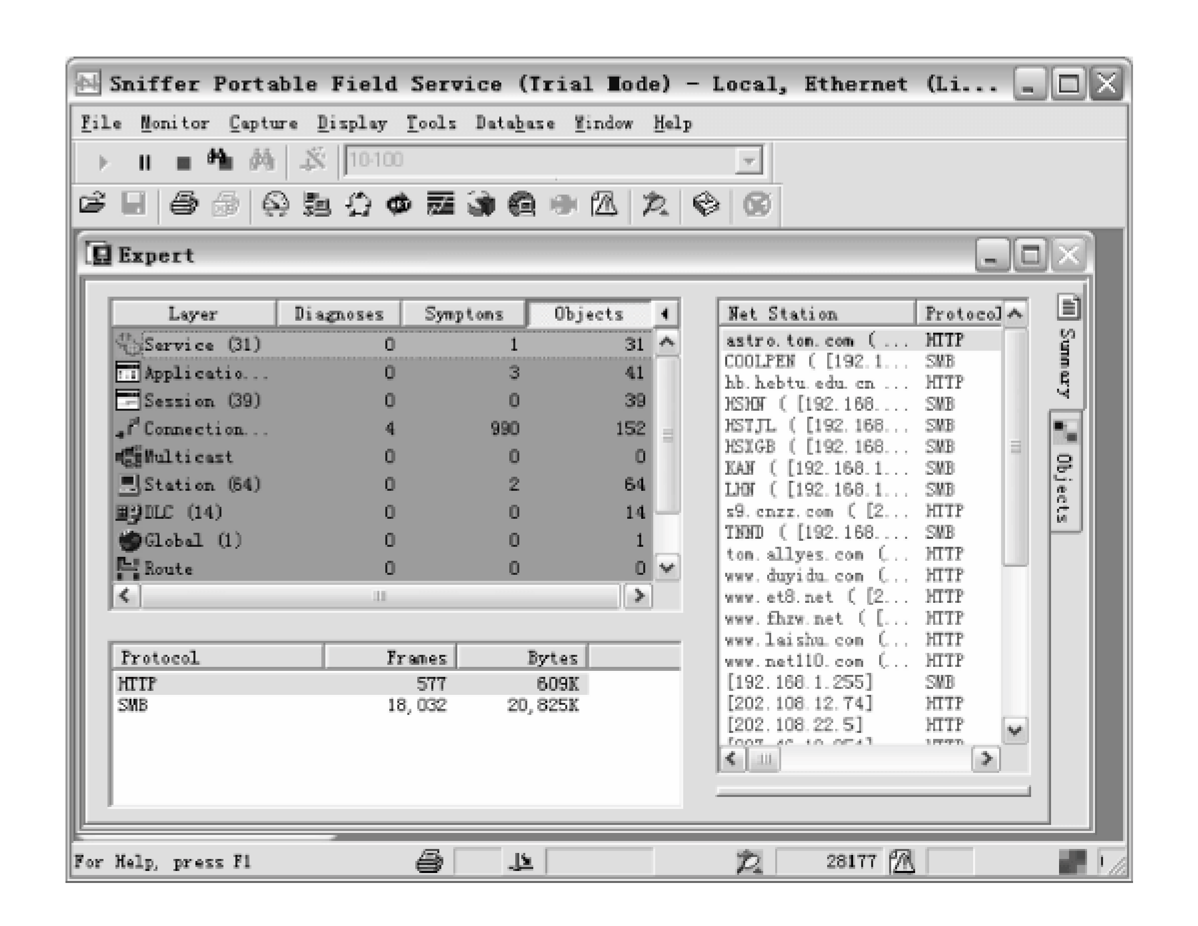


图 9-26　Expert 窗口

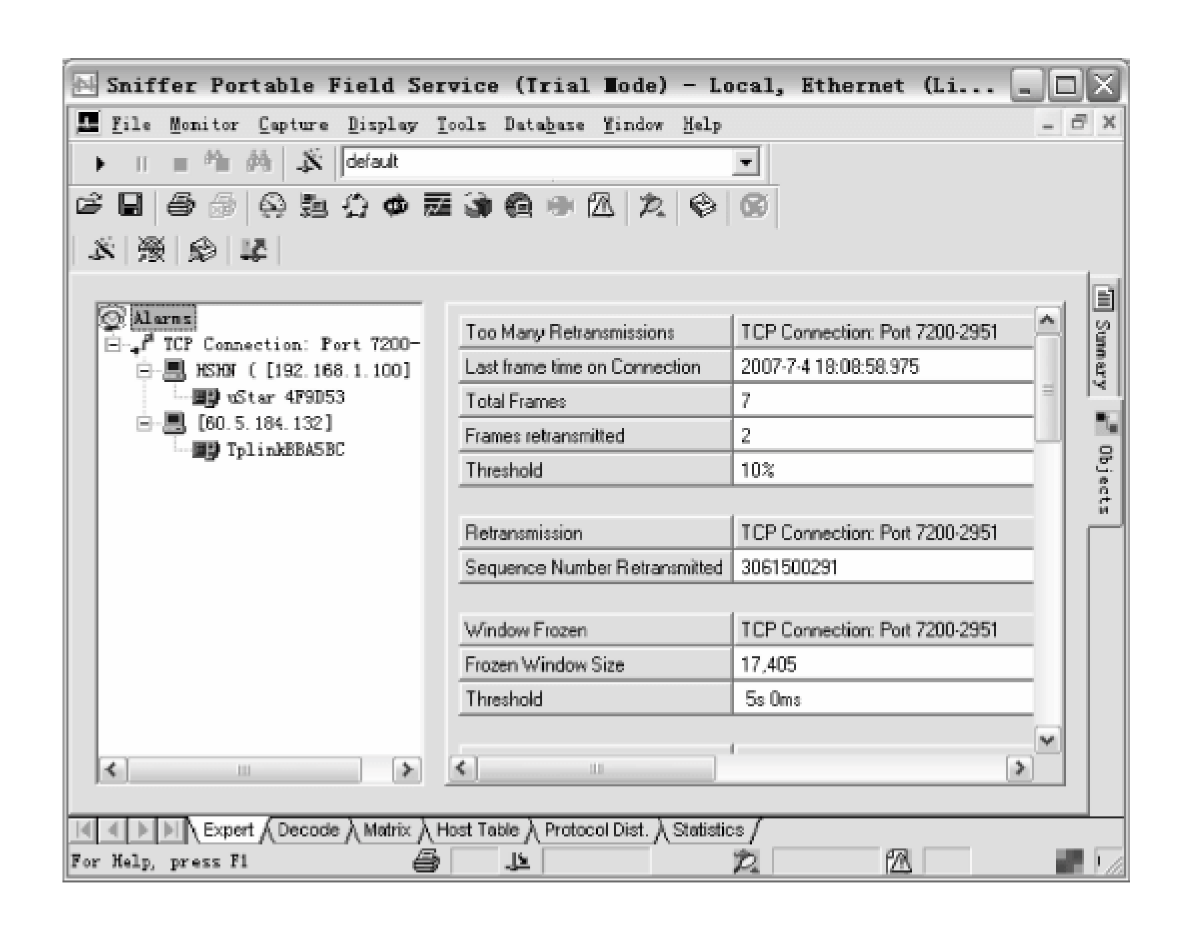


图 9-27　Objects 选项卡

(2) 查看分析捕获的数据

依次选择 Capture→Display 命令，即可查看所有捕获的内容了。选择该窗口下方的 Decode(解码)选项卡，显示图 9-28 所示的窗口，该窗口共分为 3 个部分，由上到下依次为：总结、详细资料和 Hex 窗格的内容，可以查看所捕获的每个帧的详细信息。

提示： Sniffer 所捕获的数据保存在缓冲区中。Sniffer 4.9 的缓冲区大小默认为 64MB，而 Sniffer 4.7 的缓冲区默认只有 8MB，当缓冲区满了以后就会自动停止捕获。

所捕获的数据的各部分的含义具体如下。

① DLC。在 DLC 区域中显示了捕获的帧的来源信息，包括 Source Addess(源地址)、Dest Address(目标地址)、帧大小(以字节计)以及 Ethertype(以太类型)。在这里，以太类型值为 0800，表示是 IPv4 协议。对于 IPv4 协议，它的标识符用二进制表示是 2048，十六进制表示就是 0800，十进制表示是 513，而以八进制表示是 1001。其中，Source Addess 或 Dest Address 中会显示网卡的 MAC 地址。

② IP。如果捕获的是 HTTP 协议，则 IP 区域中显示了 IP 文件头的详细内容，如

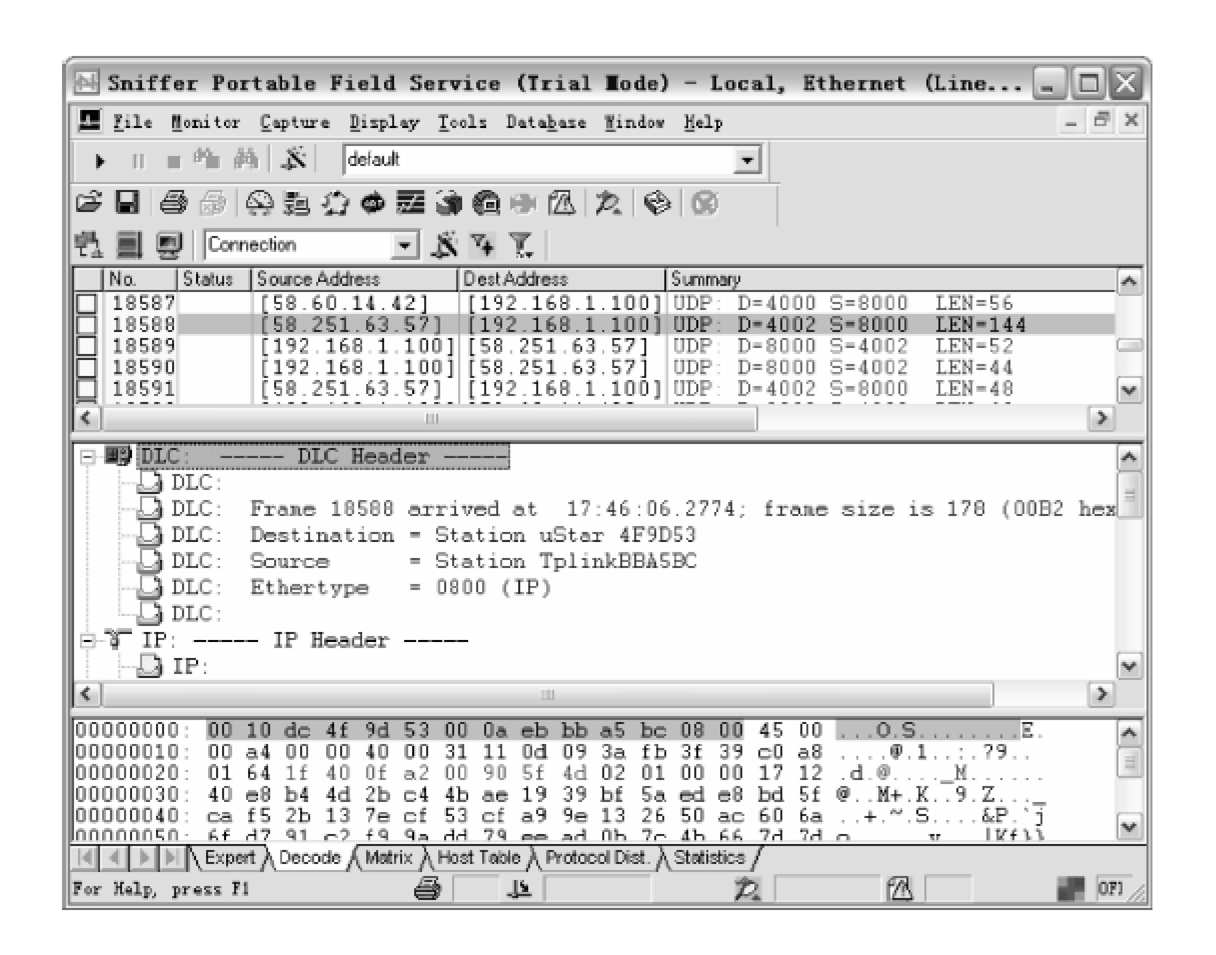


图 9-28 捕获的数据信息

图 9-29 所示，各内容含义如下。

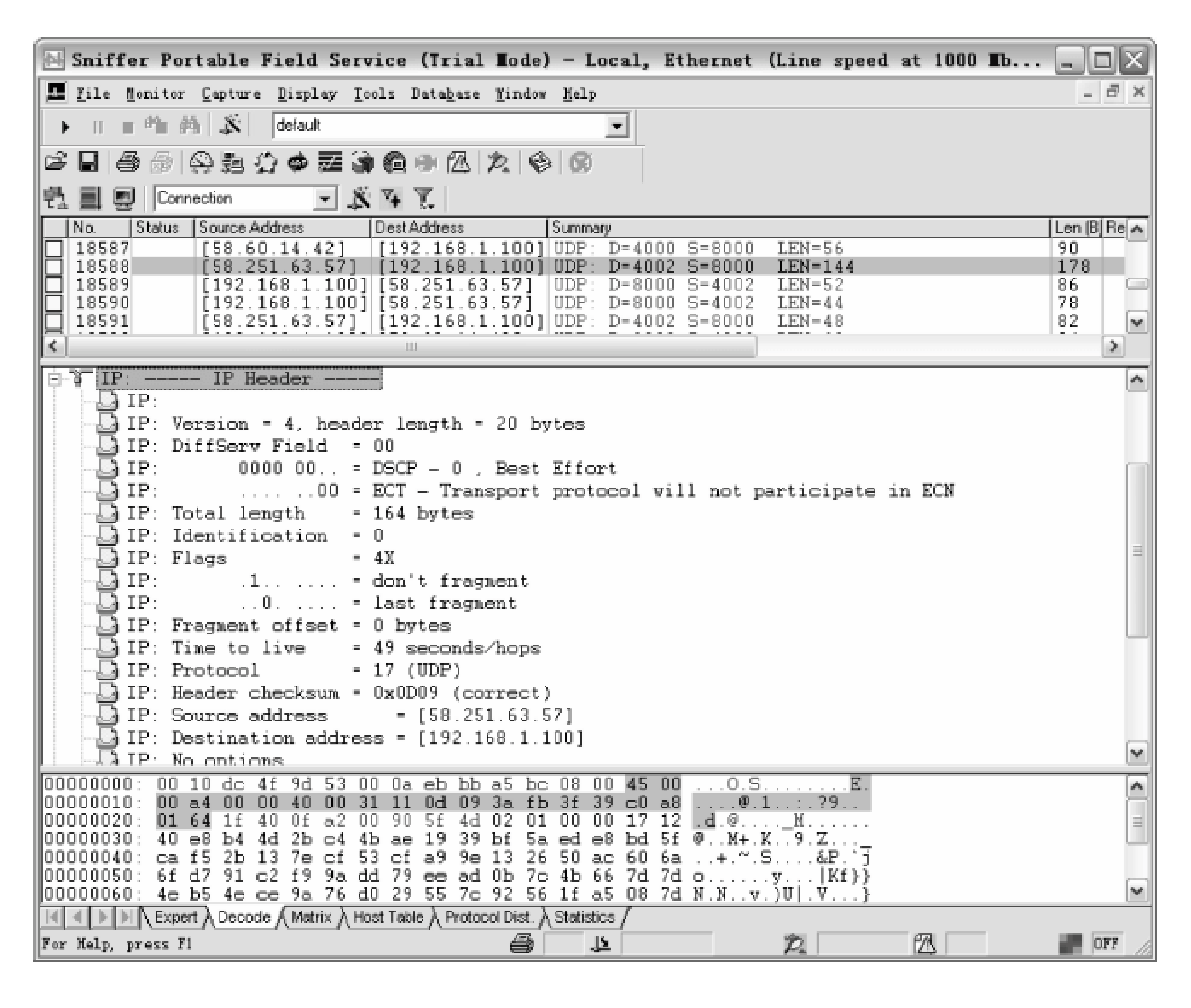


图 9-29 IP 文件头信息

- Version(版本)：版本序号为 4，代表 IPv4。
- Header length：Internet 文件头长度，为 20 个字节。
- Type of service(服务类型值)：该值为 00，会看到 Tos 下面一直到总长的部分都是 0。这里可以提供服务质量(QoS)信息。每个二进制数位的意义都不同，这取决于最初的设定，例如，正常延迟设定为 0，说明没有设定为低延迟，如果是低延迟，设定值应为 1。
- Total length(总长度)：显示该数据的总长度，为 Internet 文件头和数据的长度之和。
- Identification：该数值是文件头的标识符部分，当数据报被划分成几段传送时，接收

数据的主机可以用这个数值来重新组装数据。

- Flag(标记)：数据报的"标记"功能，例如，数据报分段用 0 标记，未分段用 1 标记。
- Fragment offset(分段差距)：分段差距为 0 个字节。可以设定 0 代表最后一段，或者设定 1 代表更多区段。这里这个值为 0。分段差距用来说明某个区段属于数据包的哪个部分。
- Time to live(保存时间)：表示 TTL 值的大小，说明一个数据包可以保存多久。
- Protocol(协议)：显示协议值，在 Sniffer 中代表 TCP 协议。文件头的协议部分只说明要使用的下一个上层协议是什么，在这里为 TCP。
- Header checksum(校验和)：这里显示了校验和(只在这个文件头中使用)的值，并且已经做了标记，表明这个数值是正确的。
- Source address(来源地址)：显示了数据的来源地址。
- Destination address(目的地址)：显示了数据访问的目的地址。

③ UDP。IP 文件头(如图 9-30 所示)一般为 TCP 或 UDP 文件头，这里为 UDP 文件头，包括下列信息。

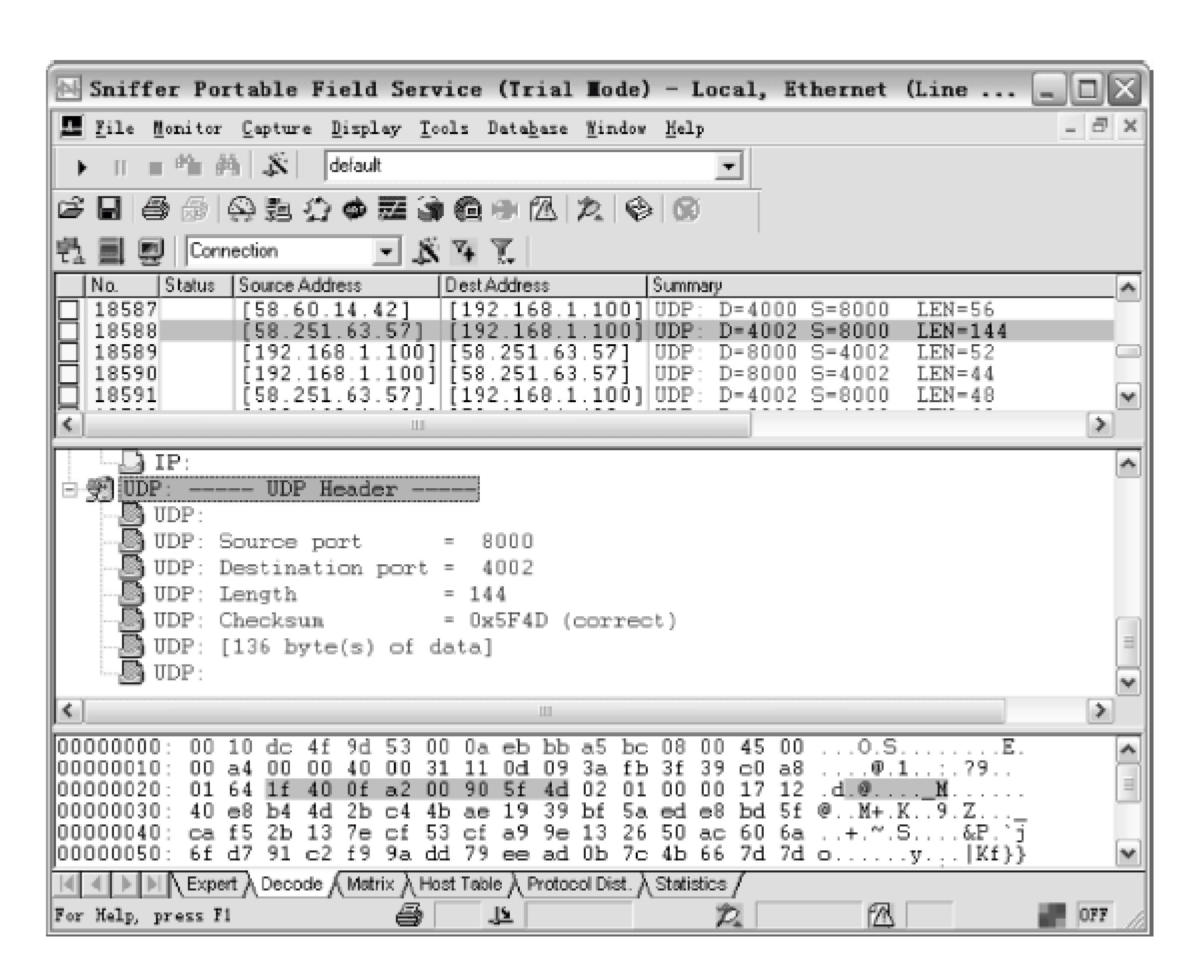


图 9-30 UDP 文件头信息

- Source port(源端口)：显示了所使用的 UDP 协议的源端口。
- Destiantion port(目的端口)：显示了 UDP 协议的目的端口。
- Length(长度)：表示 IP 文件头的长度。
- Checksum(校验和)：显示了 UDP 协议的校验和。
- Byte(s)of date：表示有多少字节的数据。

④ ARP。ARP 构架(如图 9-31 所示)中具有如下的一些信息。

- Hardware type(硬件类型)：这是一个 16 比特字段，用来定义运行 ARP 的网络的类型。每一个局域网基于其类型被指派给一个整数，例如，以太网是类型 1。ARP 可使用在任何网络上。
- Protocol type(协议类型)：这是一个 16 比特字段，用来定义协议的类型，例如，对 IPv4 协议，这个字段的值是 0800。ARP 可用于任何高层协议。

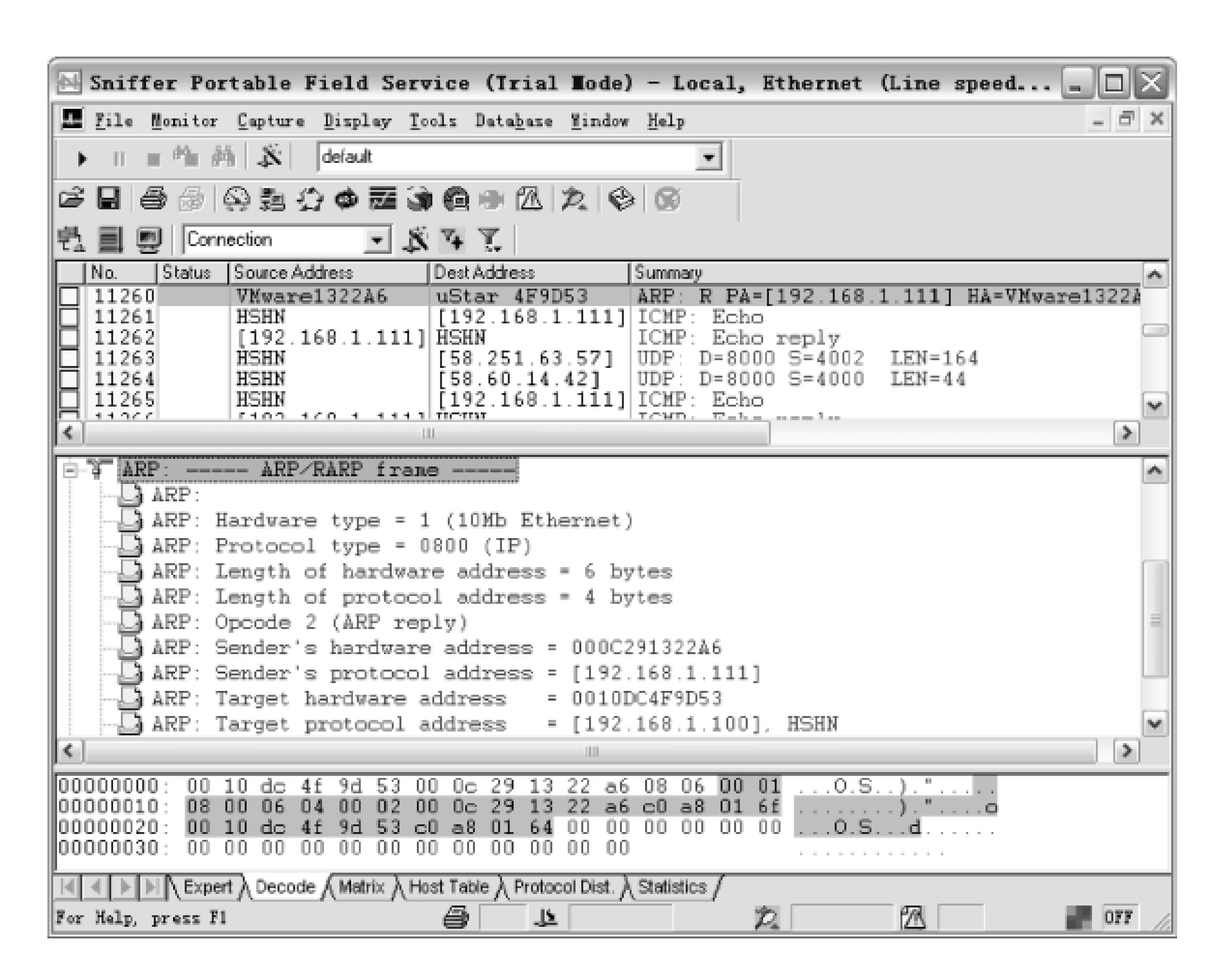


图 9-31　ARP 文件头信息

- Length of hardware address(硬件长度)：这是一个 8 比特字段，用来定义以字节为单位的物理地址的长度，例如，对以太网这个值是 6。
- Length of Protocol address(协议长度)：这是一个 8 比特字段，用来定义以字节为单位的逻辑地址的长度，例如，对 IPv4 协议这个值是 4。
- Opcode(操作)：这是一个 16 比特的字段，用来定义分组的类型。已定义了两种类型：ARP 请求第 1 步，ARP 回答第 2 步。
- Sender's hardware address(发送站硬件地址)：这是一个可变长度字段，用来定义发送站的物理地址的长度，例如，对以太网这个字段是 6 字节长。
- Sender's protocol address(发送站协议地址)：这是一个可变长度字段，用来定义发送站的逻辑(例如 IP)地址的长度，例如，对于 IP 协议，这个字段是 4 字节长。
- Target hardware address(目标硬件地址)：这是一个可变长度字段，用来定义目标的物理地址的长度，例如，对以太网这个字段是 6 字节长。对于 ARP 请求报文，这个字段是全 0，因为发送站不知道目标的物理地址。
- Target protocol address(目标协议地址)：这是一个可变长度字段，用来定义目标的逻辑地址(例如，IP 地址)的长度，例如，对于 IPv4 协议，这个字段是 4 字节长。

⑤ ICMP。ICMP 协议即 Internet 控制信息协议，是 TCP/IP 协议栈的一部分。ICMP 是一种非常强大的工具，允许报告 20 种以上不同的网络状况。首先需要创建一个新的 ICMP 过滤器，即在 Advanced 选项卡中选中 IP 列表中的 ICMP 协议，捕获足够数据后便可以进行分析。

由于 ICMP 信息封装在 IP 数据包中，而 IP 数据包又会封装在以太网帧中，如果要彻底分析一个 ICMP 数据包，就必须查看这个数据包的所有部分，即理解 3 种不同的文件头：DLC 文件头、IP 文件头和 ICMP 文件头，如图 9-32 所示。其中，ICMP 文件头包括如下内容。

- Type：ICMP Echo 有两种类型，类型 8 是请求，而类型 0 是响应。
- Code：该代码现在在 ICMP Echo 信息中并不常用，经常设定为 0。

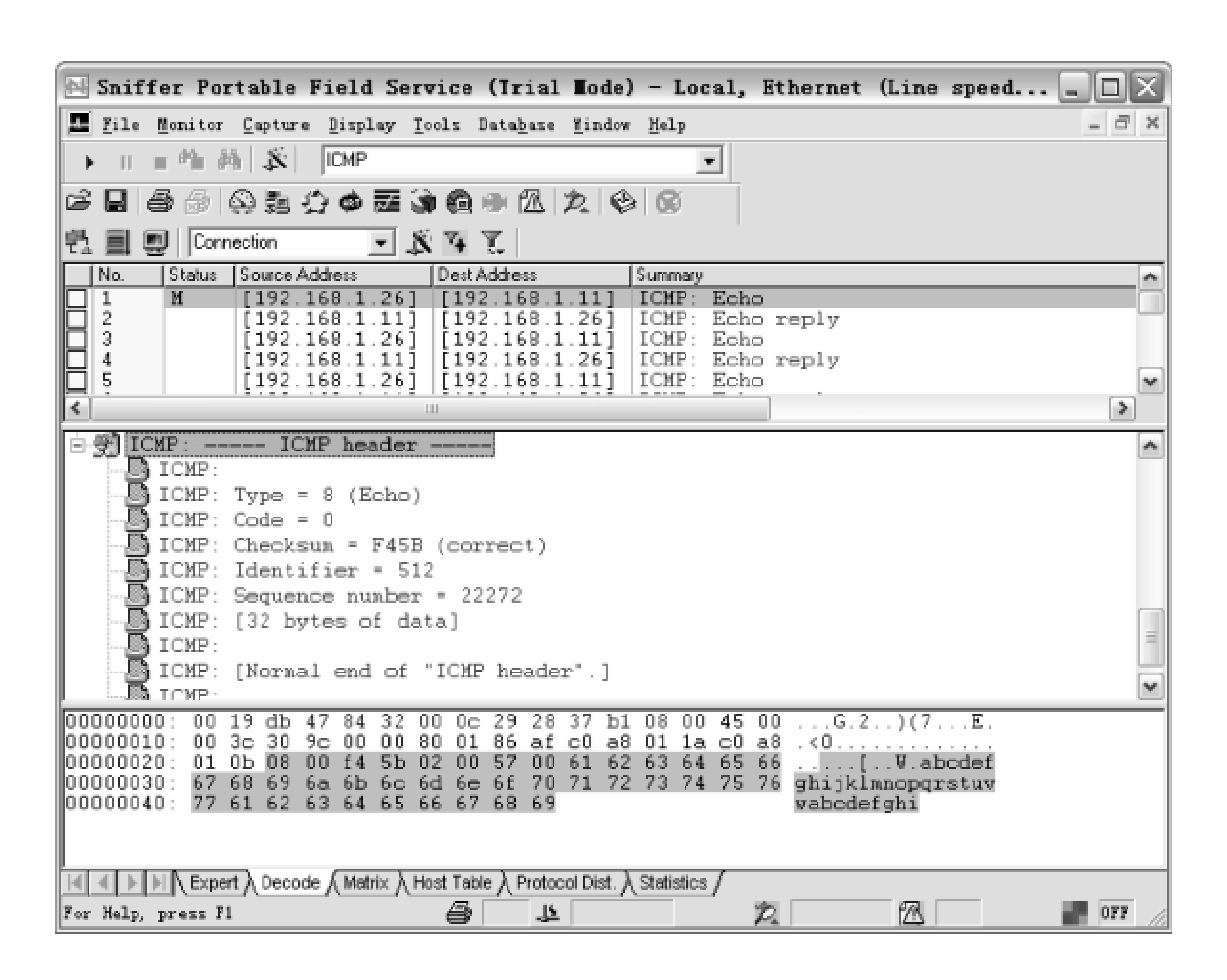


图 9-32 ICMP 文件头

- Checksum：IP 文件头校验和不能用来证明高层协议数据的完整性，所以 ICMP 信息用自己的校验和来确保数据在传输过程中没有被中断。
- Identifier 与 Sequence number：这些数字由发送方式生成，用来将响应与请求匹配在一起。

⑥ Hex。Decode 选项卡最下方为“Hex 窗格”，这里显示的内容最直观，但也难以理解。“Hex 窗格”中的信息是十六进制代码的信息集合。数据的传输是按照二进制系统为基本标准进行的，二进制数据还可以转换为十六进制、十进制和八进制的格式，在“Hex 窗格”中查看数据时，看到的就是处于传输状态的原始 ACSII 格式的数据。

⑦ Matrix。Sniffer 的矩阵功能可以直观地显示网络中各计算机之间的连接。选择窗口下方的 Matrix 选项卡，显示如图 9-33 所示，以 Matrix 方式显示了网络中各计算机之间的连接情况，默认以 MAC 地址代表计算机。这里的图形界面类似于 Sniffer 监视功能中的

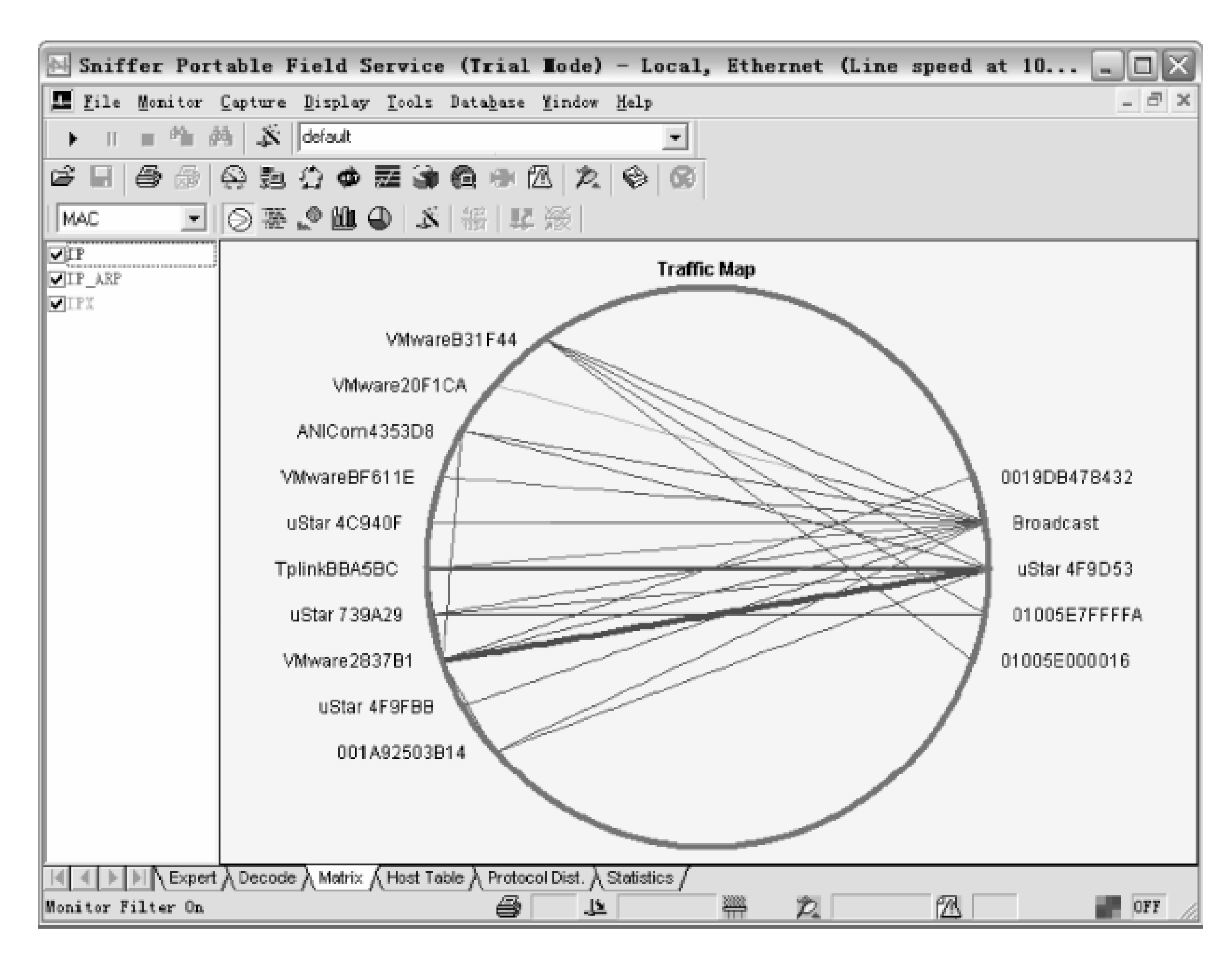


图 9-33 Matrix 图表

Matrix 界面。所不同的是，此处显示的是固定数据，即曾经捕获到的数据，而 Monitor 中的 Matrix 是不断变化的，并会随时添加即时捕获的数据。

为便于查看，可以以 IP 地址形式显示计算机。在 MAC 下拉列表框中选择 IP 选项，即可显示各计算机的 IP 地址，并使用不同颜色的连线来显示各连接所使用的不同协议，如图 9-34 所示。

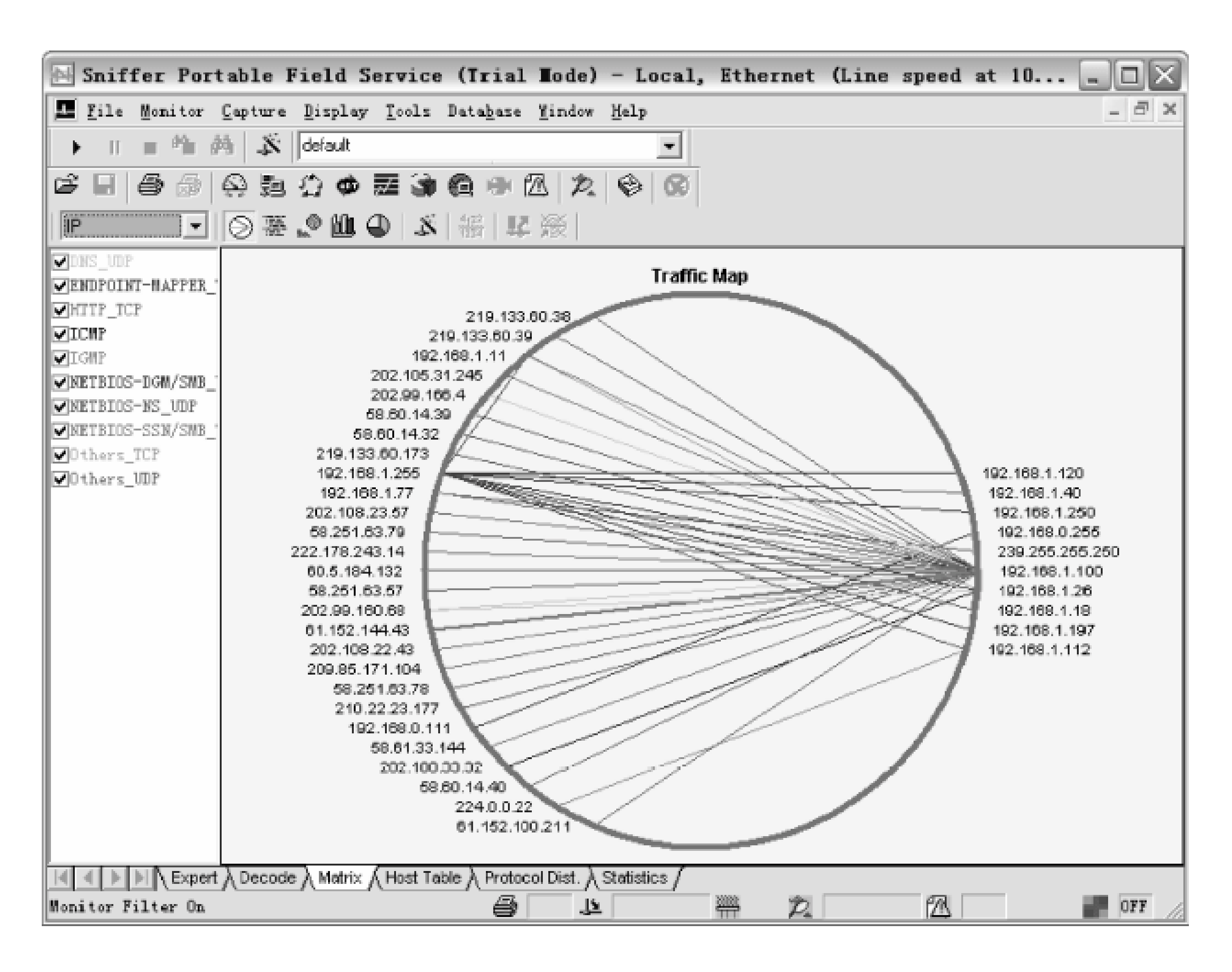
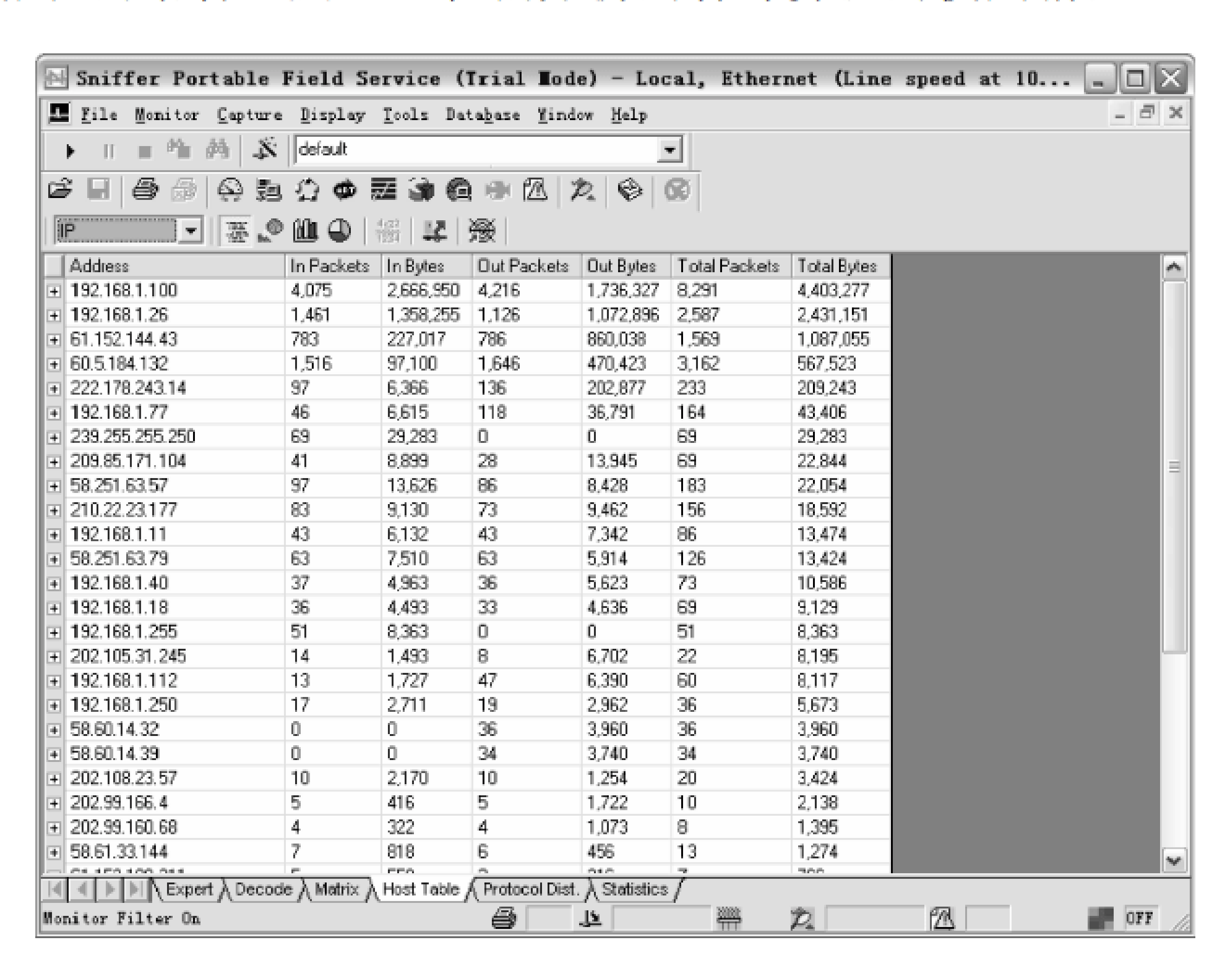


图 9-34 显示 IP 协议连接

⑧ Host Table。主机列表是一个很有用的功能，如图 9-35 所示。该功能可以清楚地显示出在该捕获过程中各计算机所传输的数据，并且可以根据所传输数据多少按顺序排列。与 Matrix 结合使用，网络管理员可以轻松分析出各计算机的使用情况。



Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
192.168.1.100	4,075	2,666,950	4,216	1,736,327	8,291	4,403,277
192.168.1.26	1,461	1,358,255	1,126	1,072,896	2,587	2,431,151
61.152.144.43	783	227,017	786	860,038	1,569	1,087,055
60.5.184.132	1,516	97,100	1,646	470,423	3,162	567,523
222.178.243.14	97	6,366	136	202,877	233	209,243
192.168.1.77	46	6,615	118	36,791	164	43,406
239.255.255.250	69	29,283	0	0	69	29,283
209.85.171.104	41	8,899	28	13,945	69	22,844
58.251.63.57	97	13,626	86	8,428	183	22,054
210.22.23.177	83	9,130	73	9,462	156	18,592
192.168.1.11	43	6,132	43	7,342	86	13,474
58.251.63.79	63	7,510	63	5,914	126	13,424
192.168.1.40	37	4,963	36	5,623	73	10,586
192.168.1.18	36	4,493	33	4,636	69	9,129
192.168.1.255	51	8,363	0	0	51	8,363
202.105.31.245	14	1,493	8	6,702	22	8,195
192.168.1.112	13	1,727	47	6,390	60	8,117
192.168.1.250	17	2,711	19	2,962	36	5,673
58.60.14.32	0	0	36	3,960	36	3,960
58.60.14.39	0	0	34	3,740	34	3,740
202.108.23.57	10	2,170	10	1,254	20	3,424
202.99.166.4	5	416	5	1,722	10	2,138
202.99.160.68	4	322	4	1,073	8	1,395
58.61.33.144	7	818	6	456	13	1,274

图 9-35 Host Table

例如，当管理员发现上网速度特别慢，而服务器又运行正常，即可通过 Sniffer 的 Host Table 和 Matrix 功能进行分析。如果在 Host Table 中发现有计算机在某段时间内传输的

数据特别多，并且在 Matrix 中显示该计算机有大量的并发连接，由此可以得出结论：该计算机很可能在使用 BT 等 P2P 软件下载文件。为避免该用户过多占用带宽，管理员即可中止该用户的下载。

（3）保存数据

使用 Sniffer 捕获数据以后，为便于日后再次进行分析或比较，应该先将其保存，以后再重新打开并分析。

当捕获结束后，依次选择 File→Save 命令，即可将当前已捕获的数据保存到硬盘上。当日后再想重新分析时，可选择 File 菜单中的 Open 命令，选择事先保存的文件即可。

9.2.2 网络协议检测工具——Ethereal

Ethereal 是一款免费的网络协议检测程序，同时支持 UNIX 和 Windows 操作系统。使用该工具可以抓取运行的网站的相关资讯，包括每个数据包的流向及其内容，并可通过操作系统语系方便地查看和监控 TCP 会话动态等。但是，Ethereal 仅仅能提供协议分析，不具备 Sniffer 的一些功能，比如监控应用程序、高级分析和捕获变形帧。

1. Ethereal 安装

Ethereal 可以运行于 Windows 9x/NT/2000/XP 等操作系统。用户可以从它的官方网站（http://www.ethereal.com/）下载，也可以从国内一些下载站点下载。在安装 Ethereal 之前，需要先安装 WinPcap 驱动程序，WinPcap 也可以从 Ethereal 的官方网站下载。Ethereal 安装比较简单，保持默认设置即可，这里不再赘述。

2. 捕获并分析数据包

Ethereal 具有数据捕获功能，可以捕获网络中各个计算机传输的数据，通过查看并分析所捕获的数据，即可了解网络的运行状况。

（1）运行 Ethereal 程序，显示图 9-36 所示的窗口，通过该窗口即可捕获网络中的数据并进行分析。

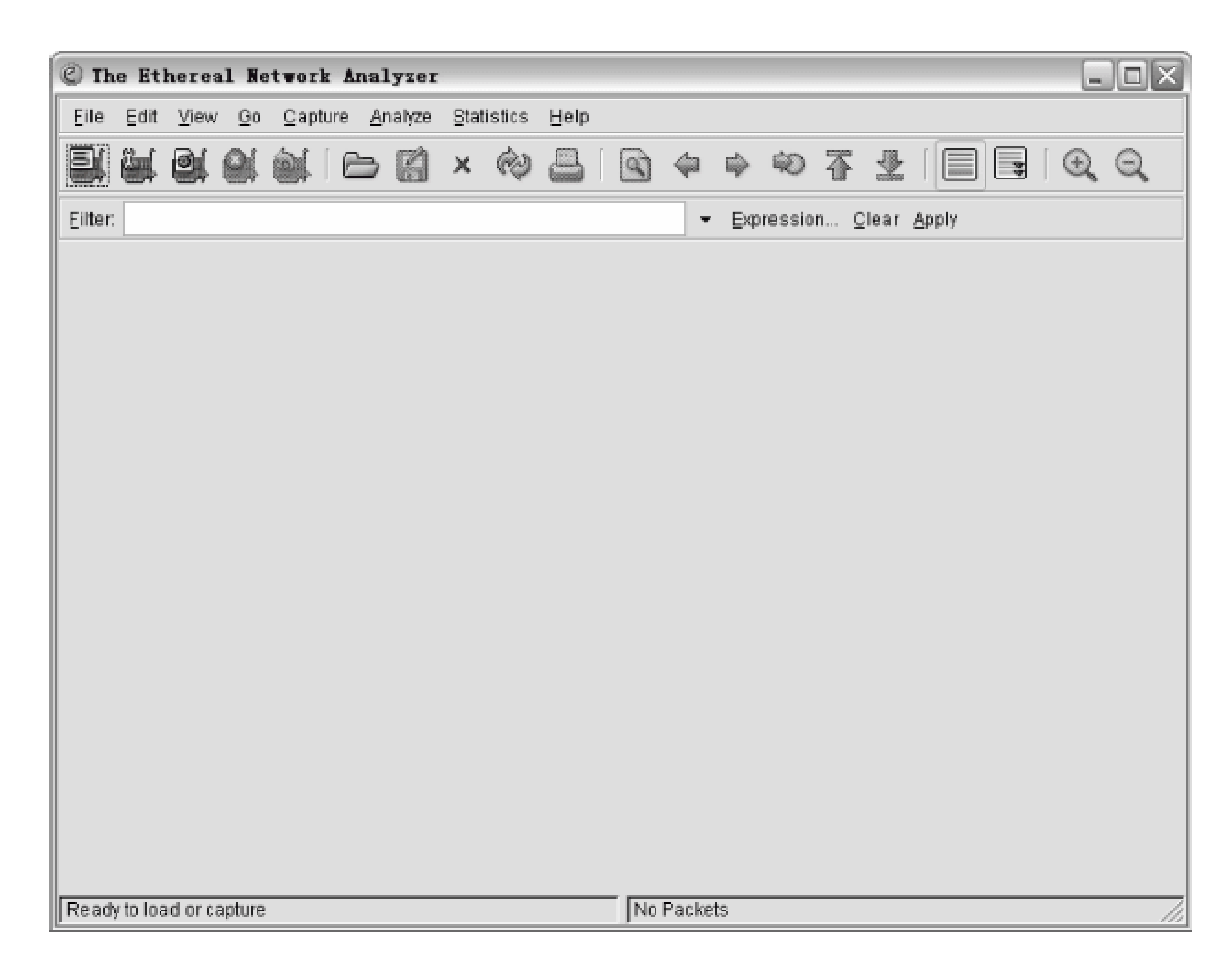


图 9-36 Ethereal 窗口

（2）依次选择 Capture→Interfaces 命令，显示图 9-37 所示的 Ethereal：Capture Interfaces 对话框，在该对话框中显示了本地计算机上所安装的网卡、网卡的 IP 地址、传输的包数量（Packets）以及包的传输速率（Packets/s）等信息。

（3）如果要捕获数据，必须先选择一个用来捕获数据的网卡，单击欲捕获数据的网卡右侧的 Capture 按钮，Ethereal 便开始利用此网卡来监控本地网络，显示图 9-38 所示的对话框，其中显示了各种协议所占的百分比。

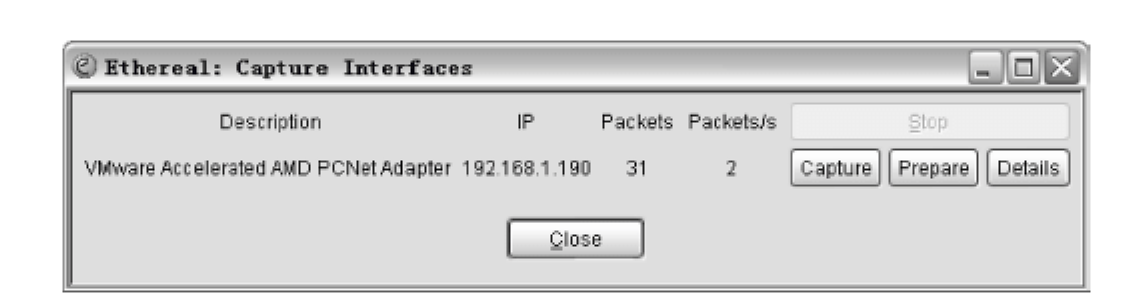


图 9-37　Ethereal：Capture Interfaces 对话框

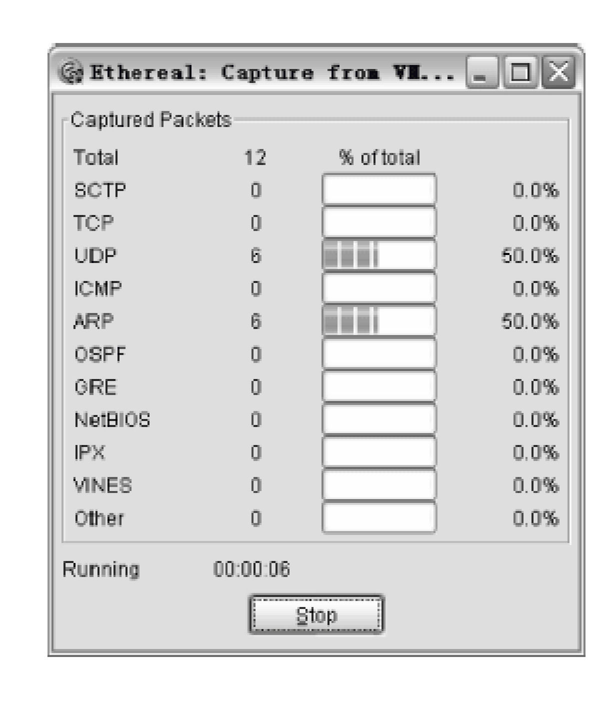


图 9-38　显示各种协议所占的百分比

（4）单击 Stop 按钮即可停止捕获，捕获到的所有数据显示在 Ethereal 主窗口中。其中包括源地址（Source）、目标地址（Destination）、使用的协议（Protocol）以及该数据包的简单信息（Info）等，如图 9-39 所示。

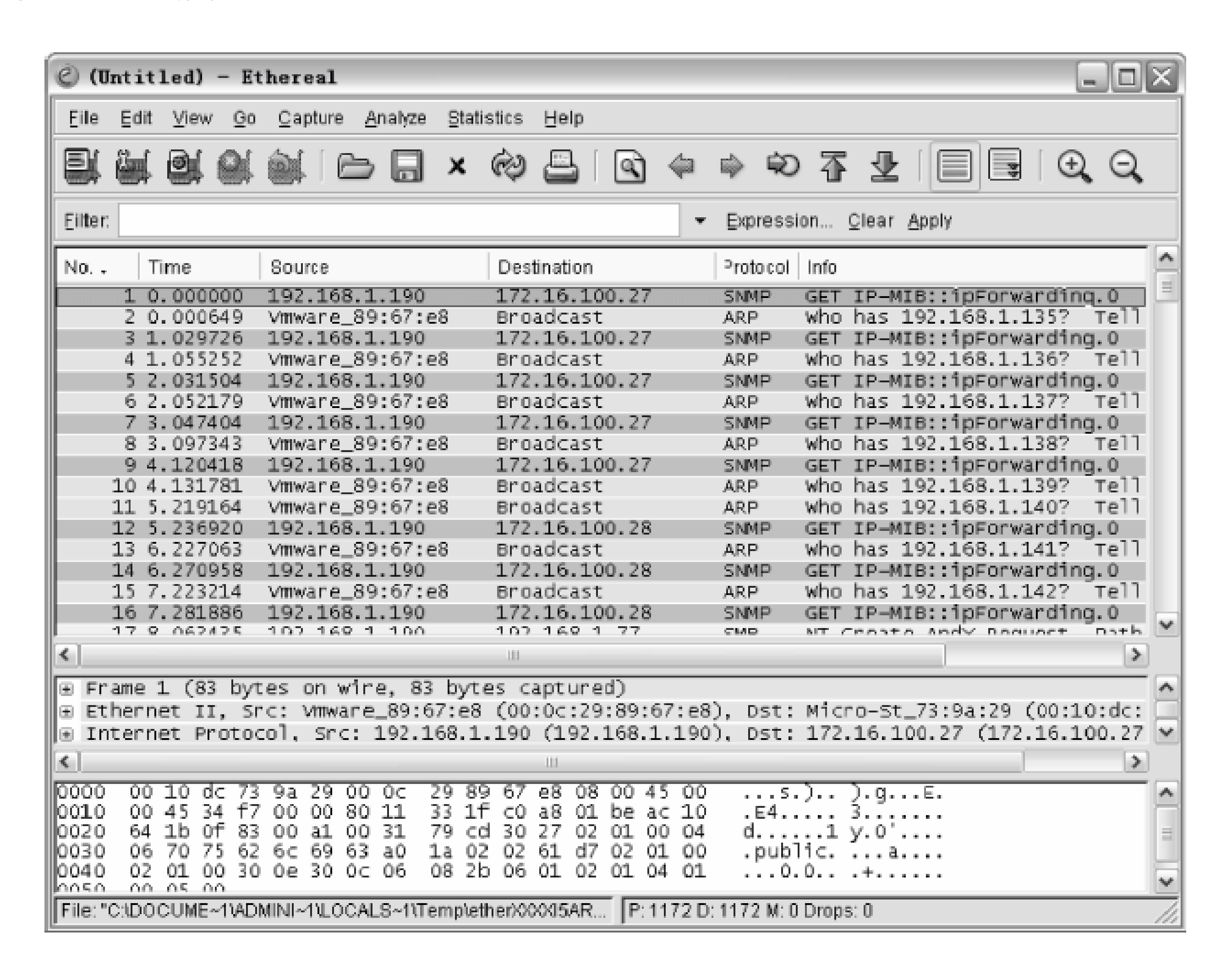


图 9-39　捕获的数据

如果需要重新捕获数据，选择 Capture 菜单中的 Start 命令即可。

3. 过滤数据包

在捕获数据时，Ethereal 会将所有协议的数据包都捕获下来，但并不是所有的数据包都是所需的，因此需要将所需的数据包过滤出来，例如，在捕获完数据后，需要分析使用 IP 协议的数据包，可在 Filter 文本框中直接输入 ip，按 Enter 键或单击 Apply 按钮，即可以在该窗

口中将使用 IP 协议的数据包全部过滤出来,而使用其他协议的数据包将全部隐藏,如图 9-40 所示。

图 9-40　过滤 IP 协议的数据包

除了直接输入要过滤的条件,所有的过滤器(Filter)都可以进行设置,单击 Expression 按钮,显示图 9-41 所示的 Ethereal: Filter Expression 窗口,可以设置要过滤的各种条件。

在 Field name 列表框中可以选择要过滤的字段名,也就是要过滤的各种协议条件,如 HTTP、IP 等,将其展开可以选择详细的字段;在 Relation 列表中选择可使用的关系;Value 文本框中用来设置数值,如 IP 地址等。

另外,可以使用如或、与、非等逻辑操作符将表达式组合起来。

(1) &&:逻辑与,如 ip.addr=10.0.0.1&&tcp.flag.fin。

(2) ||:逻辑或,如 ip.addr=10.0.0.1|| ip.add=10.0.0.2。

(3) ^^:异或,如 tr.dst[0:3]==0.6.29 xor tr.src[0:3]==。

(4) !:逻辑非,如 ! llc。

例如,要过滤 IP 地址为 10.0.0.90 的主机所接收或发送的所有 IP 报文,Filter 文本框中所使用的表达式就应该如下。

ip.addr == 192.168.1.77 and ip

然后,按 Enter 键或单击 Apply 按钮,就会过滤出 IP 地址为 192.168.1.77 的主机所发送和接收的数据包,如图 9-42 所示。

提示:在 Filter 框中输入过滤值时,如果背景是绿色,说明所输入的 Filter 值的格式是正确的,如果背景显示为红色,则说明

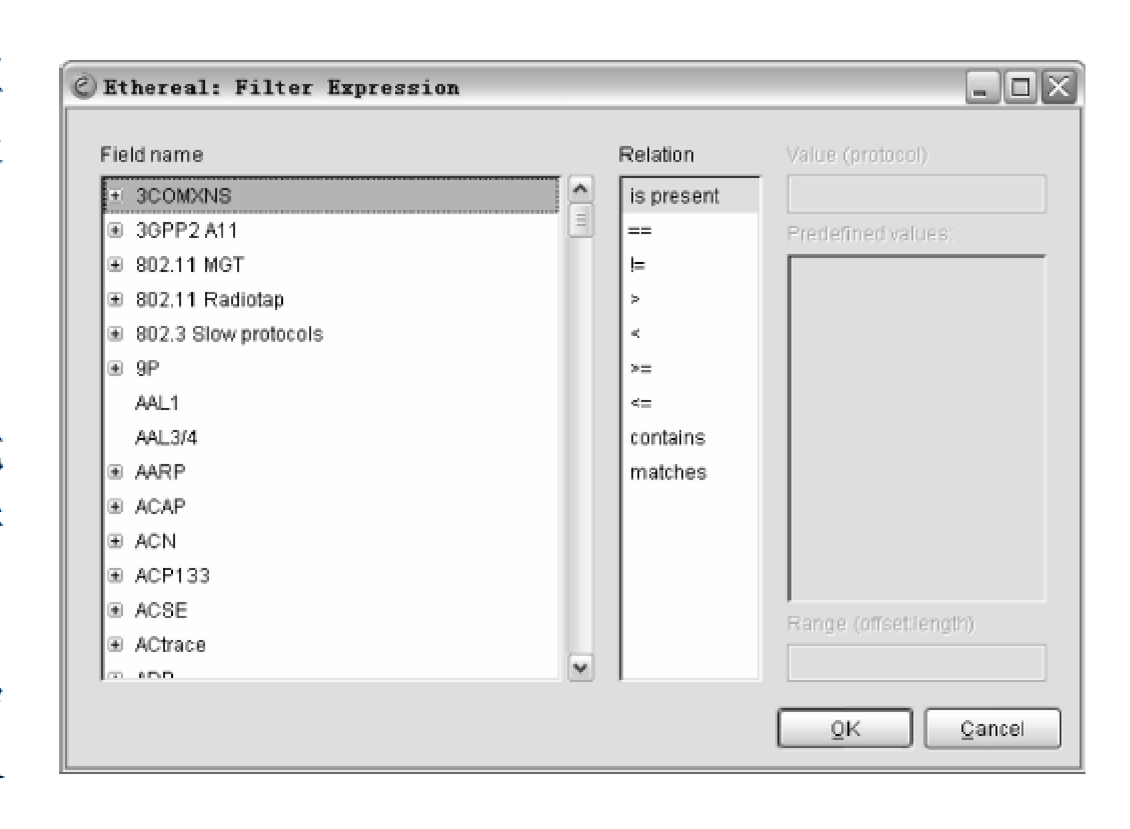


图 9-41　Ethereal: Filter Expression 窗口

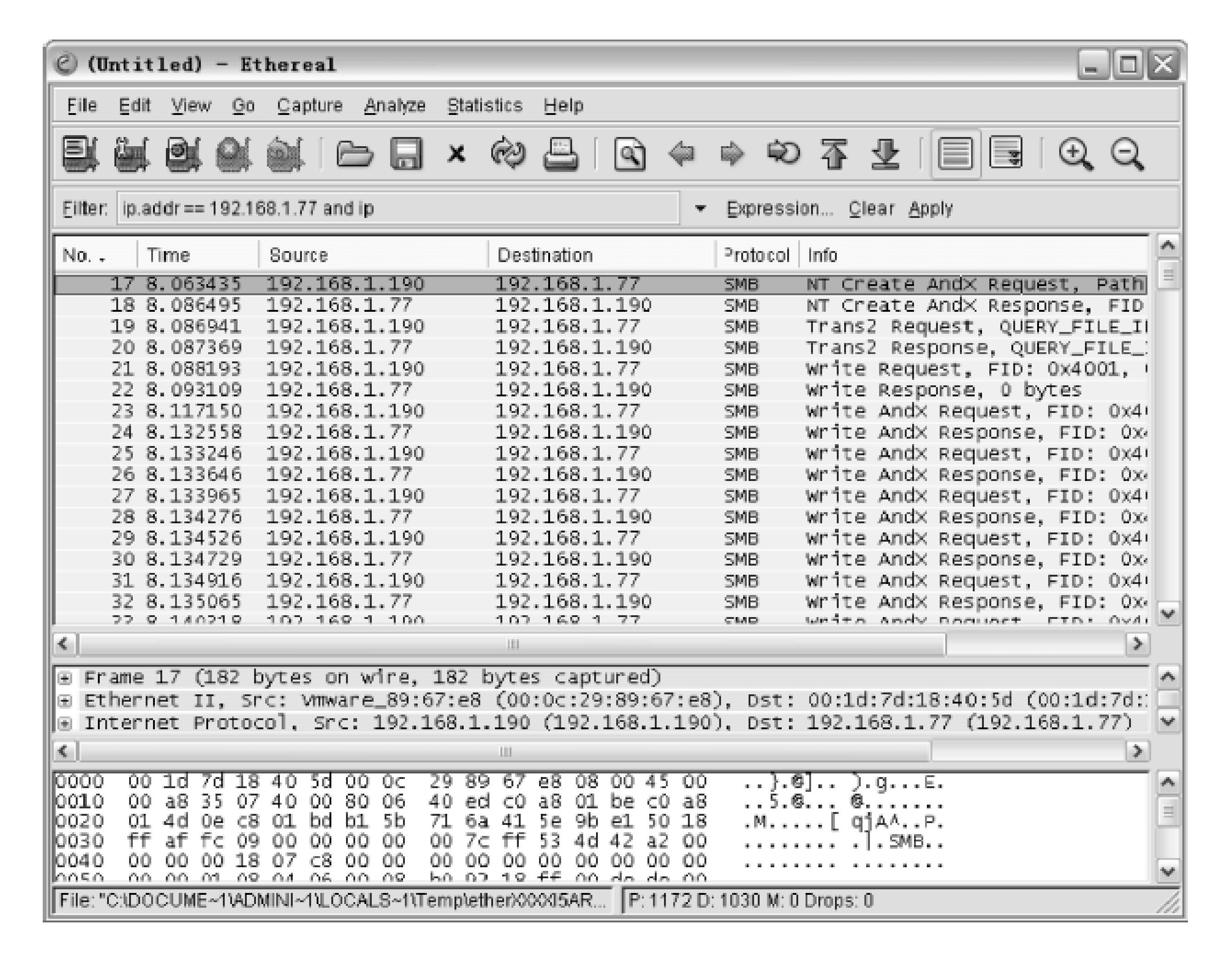


图 9-42　过滤的数据包

你设定的 Filter 值不是 Ethereal 允许的值。利用这个特点可以判断所输入的过滤器表达式是否正确。

作为网络管理员，会经常分析网络，并且经常使用各种过滤器过滤自己所需要的数据。如果有些过滤器要经常使用，但对一些复杂的过滤器，记起来太麻烦，就可以将这些过滤器保存在 Ethereal 中，当以后再使用的时候直接选择即可。

在 Ethereal 窗口中单击 Filter 按钮，显示图 9-43 所示的 Ethereal：Display Filter 窗口，在这里可以设置多个过滤器。

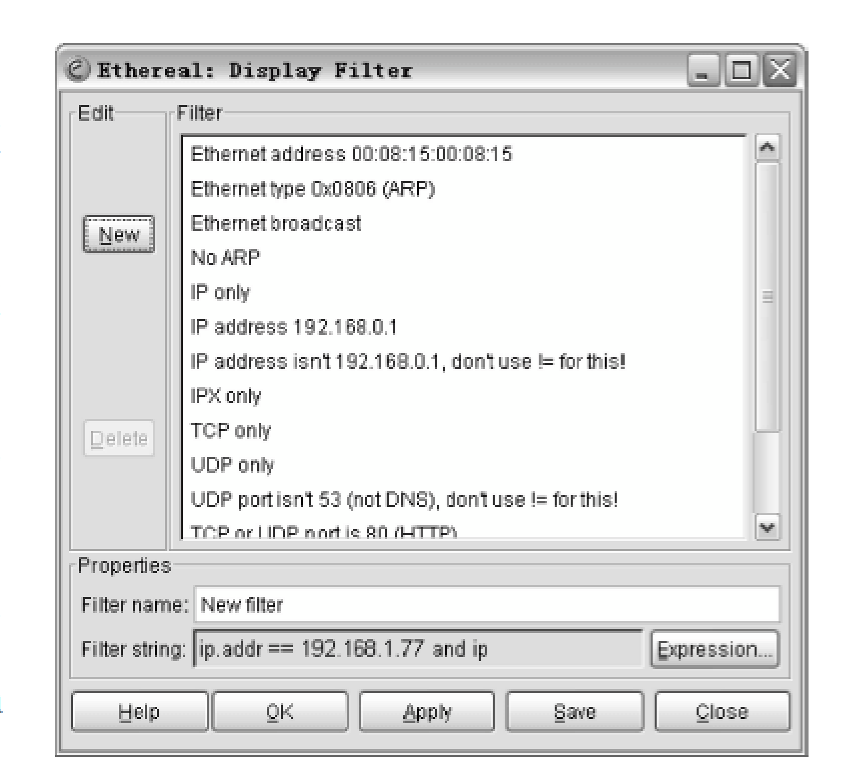


图 9-43　Ethereal：Display Filter 窗口

（1） New：单击该按钮可以添加一个新的过滤器。

（2） Filter name：设置过滤器的名称。该名称并无实际意义，主要是用来与其他过滤器区分。

（3） Filter string：设置过滤器的表达式。单击 Expression 按钮会显示 Ethereal：Filter Expression 窗口，可以设置过滤器的各种条件。

当一个过滤器设置完成以后，单击 Save 按钮即可保存在 Filter 列表框中。管理员可以设置多个不同的过滤器，当以后需要使用同样的过滤器时，直接从过滤器列表中选择就可以了。

4. 捕获设置

为了使 Ethereal 能够顺利捕获数据，必须对其进行一定的设置。

依次选择 Capture→Options 命令，显示图 9-44 所示的 Ethereal：Capture Options 窗口。其中部分选项的含义如下。

（1） Interface：选择用来捕获数据的网卡。

（2） Buffer size：设置缓冲区的大小，单位为 MB，默认为 1MB。

(3) Capture packets in promiscuous mode：是否使用混杂模式捕获数据。一般取消选中该复选框，只捕获本地计算机中发送的数据包。如果选中该复选框则使用混杂模式，捕获所有数据包。

(4) Limit each packet to：限制每个包的大小，默认为不限制。

(5) Capture Filter：设置过滤器。

在 Capture File 选项区域中，可以设置是否保存捕获的数据，如果要保存捕获的数据，可在 File 文本框中输入保存路径和文件名。

设置完成后，单击 Capture 按钮，即可使用所做的设置捕获数据。

5. 保存捕获数据

使用 Ethereal 捕获的数据可以帮助网络管理员分析网络状况，找出网络故障所在，将捕获的数据保存起来，则可以方便日后进行分析。

(1) 依次选择 File→Save 命令，显示图 9-45 所示的 Ethereal：Save file as 对话框。浏览保存位置，在"文件名"文本框中输入要保存的文件名。在 Packet Range 选项区域中可以选择要保存的数据范围，默认选中 All packets 单选按钮，即保存所有数据包。

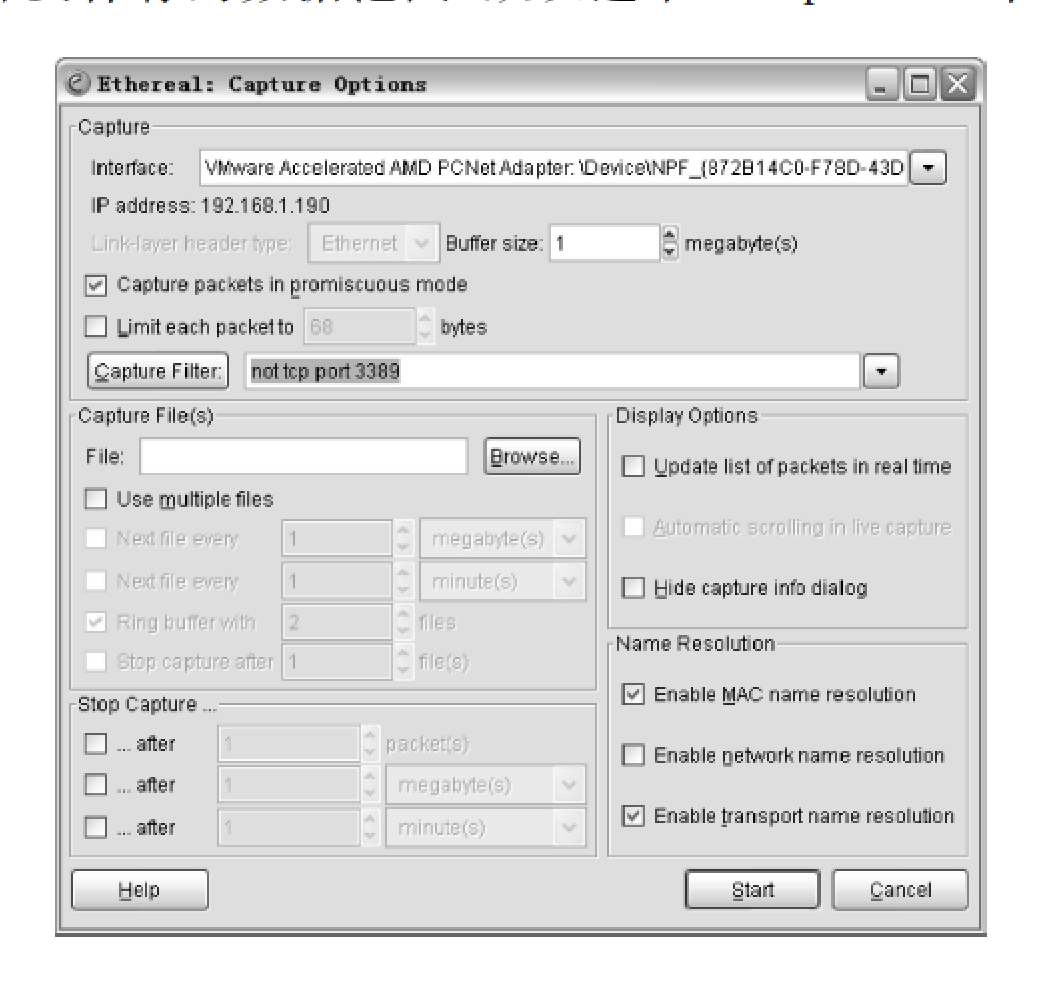




图 9-44 Ethereal：Capture Options 窗口



图 9-45 Ethereal：Save file as 对话框

(2) 单击"保存"按钮，所捕获的数据将被保存到一个文件中。

如果想查看该数据，则可在 Ethereal 窗口中依次选择 File→Open 命令，打开保存的文件即可。

9.3 IP 地址资源管理

在大多数的局域网中，IP 地址是计算机通信的唯一基础。当网络计算机数量比较多时，想要准确记忆每一台计算机的 IP 地址，显然是一件不太可能的事情。如果网络规模相当大，而且划分了 VLAN，那么网络管理员更无法准确记忆用户 IP 地址了。

9.3.1 IP Address Tracker

SolarWinds IP Address Tracker 可用于监控网络上 IP 地址的使用情况，也可用来分配

IP 地址。IP Address Tracker 是一款免费软件，适用于 Windows XP/2003/Vista/2008，该软件可以直接从其官方网站（http://www.solarwinds.com）进行下载，安装完成后即可使用。

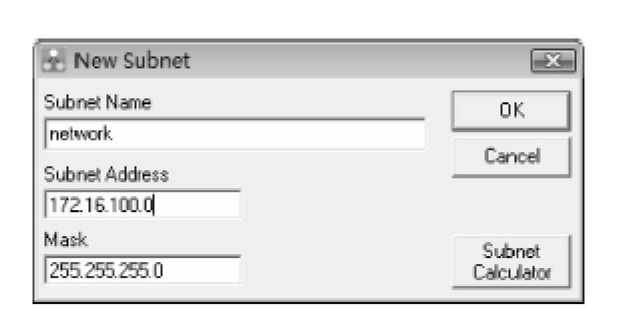


图 9-46　New Subnet 对话框

1. 扫描子网

扫描子网的步骤如下。

（1）依次选择 Subnet→New 命令，显示图 9-46 所示的 New Subnet 对话框。在 Subnet Name 文本框中，输入所要扫描的网络名称，在 Subnet Address 和 Mask 文本框中，输入所要扫描网络的网络段和子网掩码。

（2）单击 OK 按钮，即可开始扫描，扫描完成后显示图 9-47 所示的扫描结果窗口。

2. 标记 IP 地址

默认情况下，扫描完成后只将 IP 地址标记为已使用和可用两种状态，并不会将预留的 IP 地址标记出来，此时，为了便于管理和查看，可以手动标记预留的 IP 地址。

在扫描结果中，右击可用的 IP 地址，在快捷菜单中选择 Mark Select Address as Reserved 命令，即可将该 IP 地址标记为紫色，如图 9-48 所示。

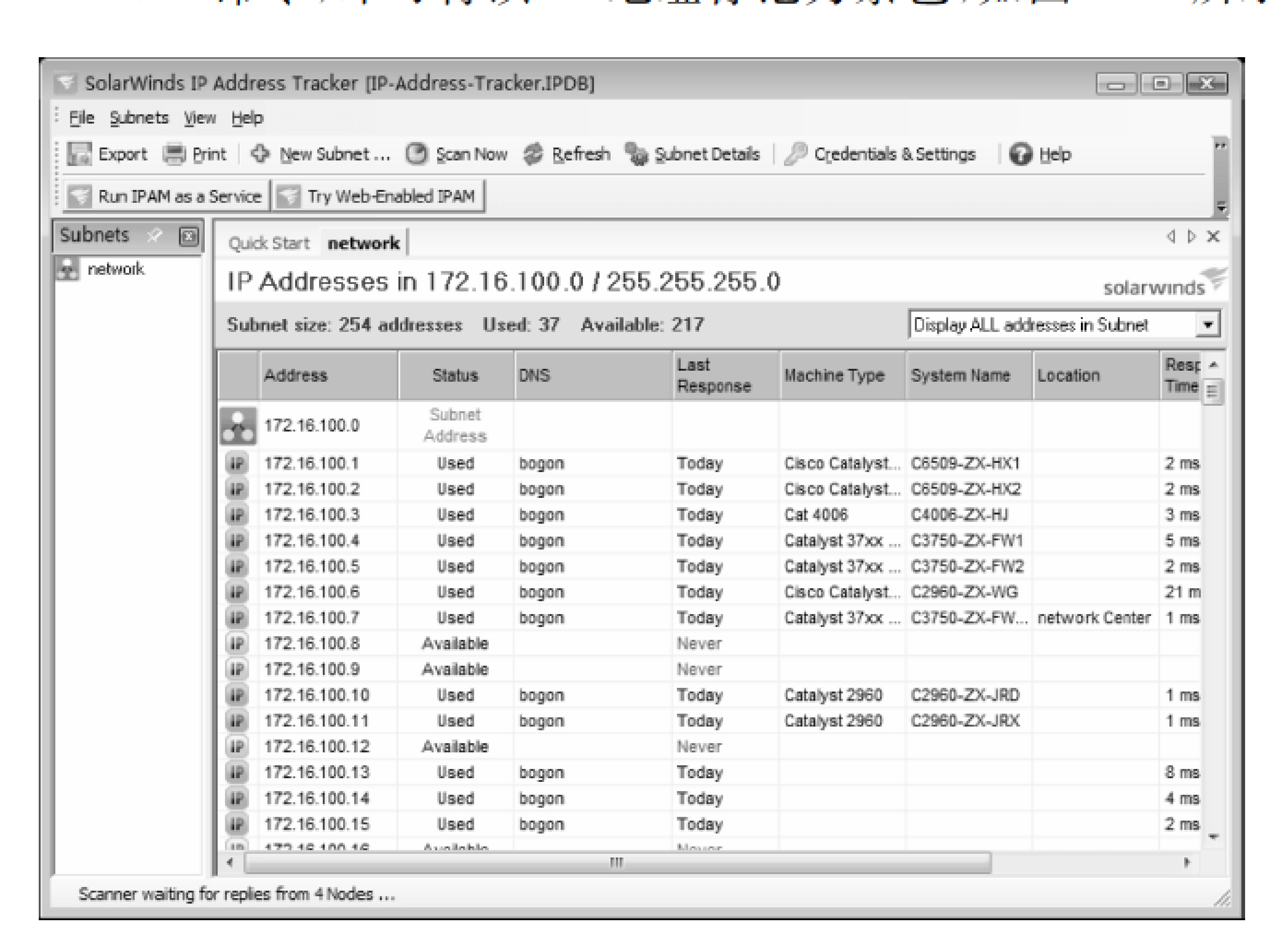


图 9-47　扫描结果



图 9-48　标记 IP 地址

3. 凭据设置

依次选择 File→Credentials&Settings 命令，显示图 9-49 所示的 Network/Scanner Settings 对话框。在 Community Strings 选项卡中，选中 Enable SNMP discovery 复选框，启用 SNMP 发现功能，在空白文本框中，输入当前网络中所使用的 SNMP 字符串，单击 Add 按钮，添加该字符串。另外，还可以根据需要设置 SNMP 字符串的顺序，选中 SNMP 字符串，单击 ✚ 按钮或 ✚ 按钮调整即可。

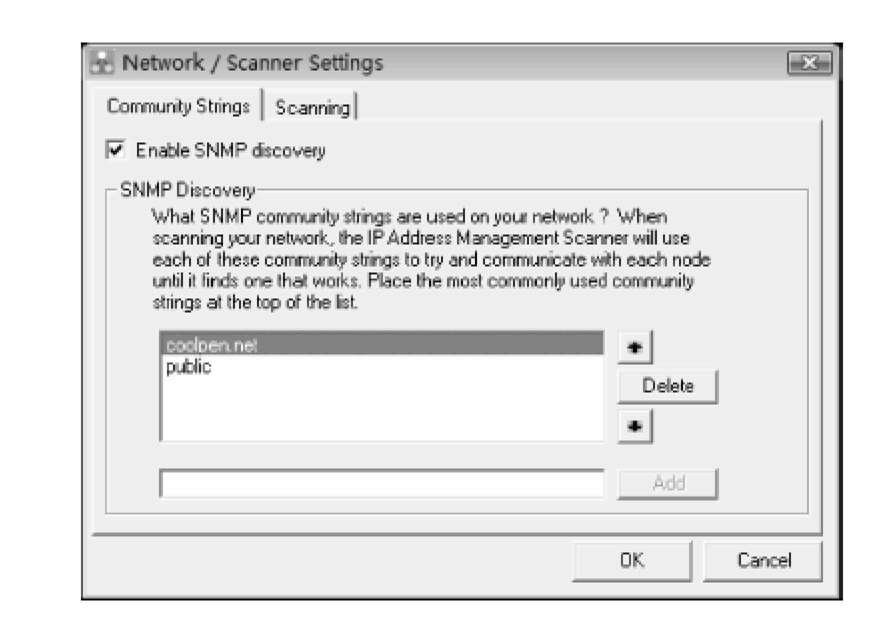


图 9-49　Network/Scanner Settings 对话框

选择图 9-50 所示的 Scanning 选项卡，根据需要拖动滑块设置所需的值，具体内容包括每个

IP 地址所发送的 Ping 包的数量、发送 Ping 包的时间间隔、Ping 包的超时时间等。

4. 导出扫描结果

IP Address Tracker 扫描完成后，可以将信息导出到其他工具，通过导出、复制和粘贴功能，还可以打印发现的信息。

依次选择 File→Export 命令，显示图 9-51 所示的 Select the Fields you would like included 对话框，根据需要选择所要导出的内容，主要包括 IP 地址、DNS 名称、系统名称等。

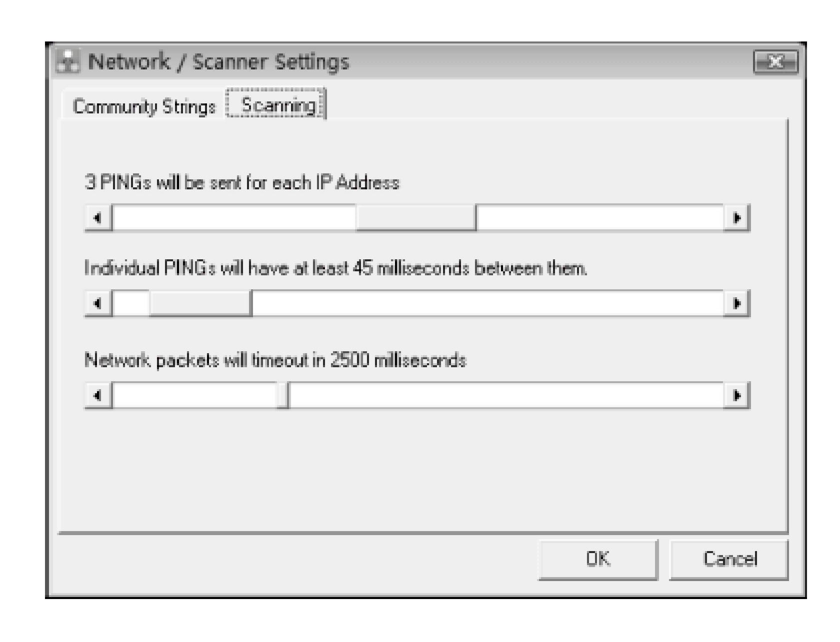


图 9-50 Scanning 选项卡

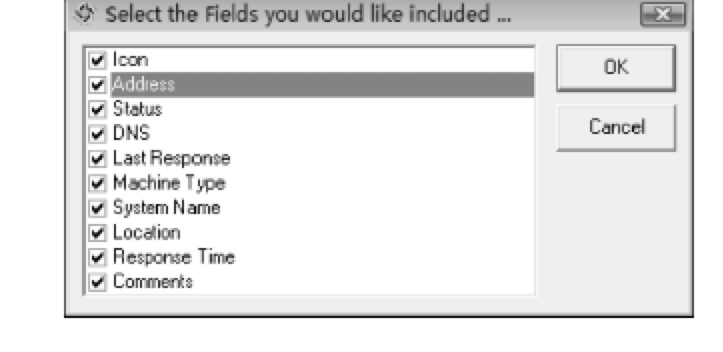


图 9-51 Select the Fields you would like included 对话框

单击 OK 按钮，根据提示设置导出文件的路径及名称即可。

9.3.2 子网计算工具

子网计算工具可以通过 IP 地址和子网掩码来计算子网内的可用 IP 地址，并且可以分别用二进制和十进制来表示。使用该工具还可以测试网络内所使用的 IP 地址和子网掩码是否正确。子网计算工具是免费的绿色软件，不需要安装，下载后即可使用。

1. 计算子网内的可用 IP 地址

运行子网计算工具，显示图 9-52 所示的“子网计算工具 V1.1”窗口，其中各选项的作用如下。

（1）请输入主机 IP：输入网络内已知的任意一个 IP 地址。

（2）请选择掩码位数：通过拖动滑块可以选择掩码位数，并在“网络掩码”中可以看到该位置的掩码 IP 地址。

（3）子网可用 IP 地址：此处用来显示计算出的网络内可用的 IP 地址范围。

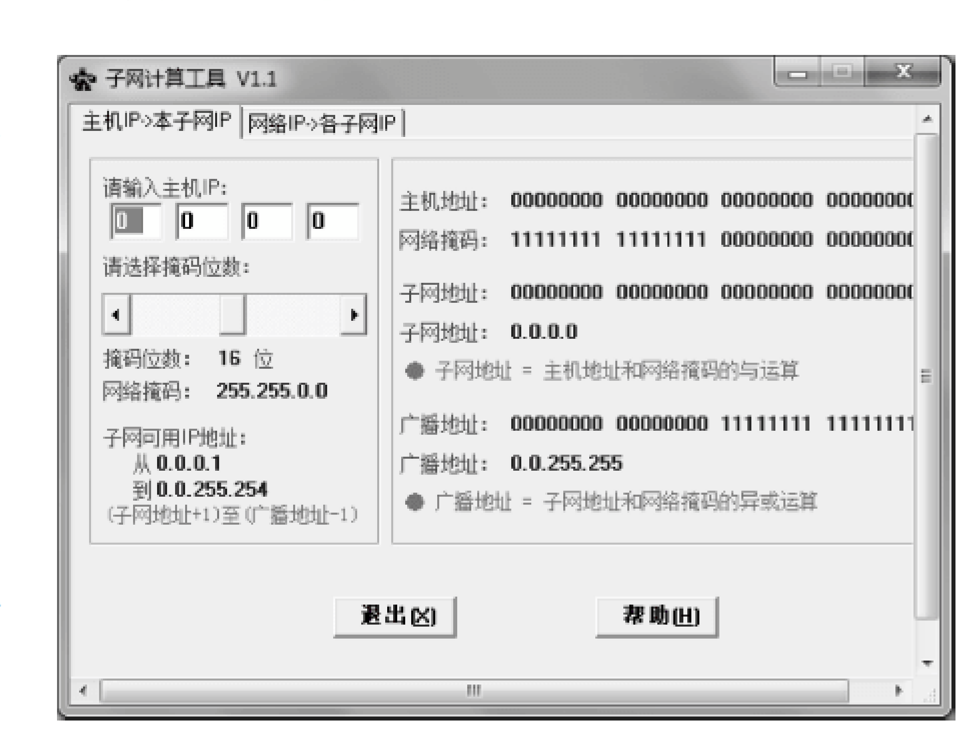


图 9-52 “子网计算工具 V1.1”窗口

在软件主窗口的右侧区域，会以二进制的形式显示网络地址和子网掩码。除显示输入 IP 地址段外，还会显示所输入某个具体的 IP 地址的二进制数值，例如，网络内的某台计算机的 IP 地址为 192.168.1.10，子网掩码为 255.255.255.192，如果想要知道该子网内的可用 IP 地址范围，可在“请输入主机 IP”文本框中输入 IP 地址 192.168.1.10，在“请选择掩码位数”中用鼠标拖动滑块，选择网络掩码为 255.255.255.192。此时，就会在“子网可用 IP 地址”中显示出该网络内的可用 IP 地址，为 192.168.1.1～192.168.1.62，如图 9-53

所示。

在该窗口右侧，除了显示出各个 IP 地址和网络掩码的二进制数值外，还显示出了子网地址和广播地址。实际上，子网地址加上 1，广播地址减去 1，就是子网可用 IP 地址。

2. 划分子网

在局域网中，可能经常会遇到划分子网的情况发生，例如添加新设备、网络改造等。使用子网计算工具，可以轻松地对所拥有的网络地址进行子网划分。

例如，现在有一个网络段为 192.168.17.x，想把它划分为几个子网。首先，在子网计算工具中选择“网络 IP->各子网 IP”选项卡，在“请输入要规划的网络地址”文本框中，输入要划分的网络地址 192.168.17.0，在“要划分的子网数量”下拉列表框中选择要划分为几个网段，这里选择 4。然后单击“计算”按钮，即可将该网络分成 4 个子网，并在右侧“各网络主机 IP 地址范围”列表框中显示出各个网段的 IP 地址，并显示出子网掩码和每网段主机数，如图 9-54 所示。



图 9-53 子网计算实例



图 9-54 划分子网实例

9.3.3 IP 地址管理——IPMaster

IPMaster 是一款对 IP 地址进行管理的软件，使用该软件可以提高管理员的工作效率，在大型网络中，使用该软件可以有序和高效地实现大中小型企业网 IP 地址的分配和管理。该软件主要包括如下功能：IP 地址分配、自动子网计算、掩码计算、子网划分、网段扫描、主机监控、Ping、TraceRoute、Telnet、Netsend 等。

1. 主要功能

IPMaster 软件是一款绿色软件，下载解压后即可直接运行。

(1) 运行 IPMaster 软件程序，显示图 9-55 所示的“登录”对话框，提示输入登录密码，默认密码为空。



图 9-55 “登录”对话框

(2) 单击“确定”按钮，即可打开图 9-56 所示的软件窗口。整个界面分为 4 部分：左边树状显示的是 IP 拓扑；右边上半部分显示的是子网或主机的属性；右边下半部分是子网的内容；下面是提示信息。不同类型的子网会用不同颜色的图标显示。



图 9-56　显示工作界面

IPMaster 软件主要功能介绍如下。

(1) 新建管理网段。

(2) 子网自动划分功能：在可再分类型的节点下，输入所需子网数、子网中的主机数或掩码，系统会自动规划子网，系统在规划时会自动跳过网段中已分配和保留类型的子网。

(3) 子网手工划分功能：在可再分类型的节点下，可根据子网的 IP 地址和掩码，手工划分子网。

(4) 删除功能：可删除指定的子网。

(5) 主机相关功能：Ping、Traceroute、Telnet、Netsend，其中 Netsend 功能只适用于已启动 Messenger 服务的 Windows 主机。

(6) 查找功能：可根据子网标识、主机 IP 地址或名称进行查询，需要注意的是，当按照名称查找时，应注意大小写。

(7) 保存功能：可以保存地址库划分信息，下次系统运行时会自动加载显示。

(8) 打开功能：用户可以打开扩展名为.adl 的地址库信息文件，并将其显示在窗口中。

(9) 输出功能：用户可以根据自己的实际需要，将地址库信息输出到 Excel 文件中。

(10) 修改恢复功能：当修改错误或失败时，可以撤销或重做最后所做的子网划分操作。

(11) 扫描功能：可以自动扫描已分配类型子网中所有的主机的名称、MAC 地址和使用人。

(12) 监控功能：用户可监控指定主机的运行情况，当该主机关闭时，可以自动报警，并且报警记录会自动保存在可执行程序所在目录中的“告警记录.log”文件中。

(13) 多种子网显示方式：用户可以根据自己的需要选择合适的子网显示方式，软件所包括的显示方式具体包括如下内容：“显示已分配与可再分网段”、“显示全部网段”、“显示已分配网段”、“显示未分配网段”、“显示保留网段”等，系统默认的显示方式是“显示已分配与可再分网段”。

(14) 密码功能：软件提供了密码登录功能，用户可以根据自己需要设置密码，软件初

始密码为空。

2. 新建管理网段

新建管理网段的步骤如下。

（1）在 IPMaster 软件主窗口中，依次选择“文件”→“新建管理网段”命令，显示图 9-57 所示的“新建管理网段”对话框。根据需要输入“网段名称”和“网段地址”，系统会根据地址类型自动确定网络掩码，并自动显示此“网段类型”、“子网 ID”、“地址范围”等信息。

（2）单击“确定”按钮，系统将会在树状拓扑图的 IPMaster-Root 节点下新建一个网段，如图 9-58 所示。



图 9-57　显示输入网段的信息



图 9-58　显示建立成功的网段

注意：通过此菜单新建的网段都会被分配在 IPMaster-Root 节点下，成为 IP 地址库的根，其节点类型默认为“可再分”。

3. 子网自动划分

使用软件提供的自动划分子网功能，可以让系统自动划分子网。

（1）在 IPMaster 主窗口右侧，右击可再分类型的管理网段，在快捷菜单中选择“划分”命令，显示图 9-59 所示的“划分子网”对话框，选中“自动划分”单选按钮。

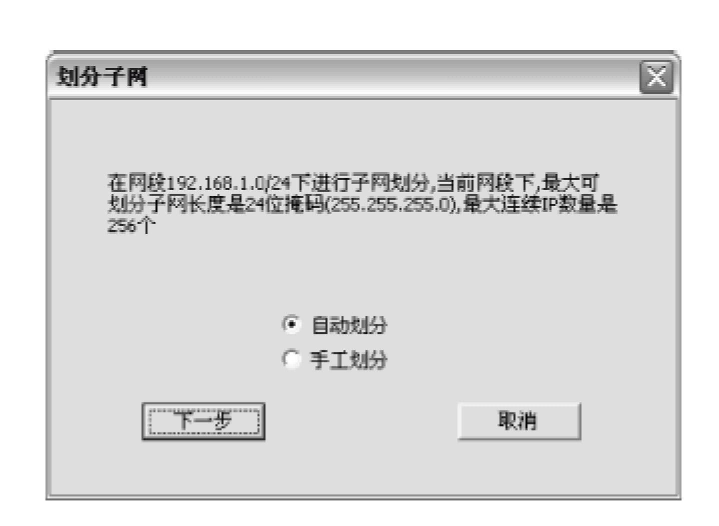


图 9-59　“划分子网”对话框

（2）单击“下一步”按钮，显示图 9-60 所示的“自动划分”对话框。在该对话框中，分别输入“划分的子网数量”、“子网中的主机数”或“子网掩码”等信息。

（3）单击“下一步”按钮，系统会自动规划生成子网，如图 9-61 所示。此时，在系统自动规划过程中，会自动跳过所规划网段中已分配和保留的子网。



图 9-60 “自动划分”对话框



图 9-61 “确认”对话框

注意：默认情况下，系统生成的子网类型是“已分配”，用户也可根据需要修改子网的类型，输入子网的名称或取消划分某个子网(去掉子网前的 check box 标签)。

(4) 单击“确定”按钮，系统即可按要求在指定的节点上生成子网。

4. 子网手工划分

除使用软件的子网自动划分功能，还可以使用手动设置的方式划分子网。使用手工划分方式，可以自定义设置名称、IP 地址、子网掩码、子网类型等内容。

(1) 在 IPMaster 主窗口右侧，右击可再分类型的管理网段，在快捷菜单中选择“划分”命令，显示图 9-62 所示的“划分子网”对话框，选中“手工划分”单选按钮。

(2) 单击“下一步”按钮，显示图 9-63 所示的“手动划分”对话框。在该对话框中，分别输入欲划分子网的“名称”、“IP 地址”、“子网掩码”和“子网类型”等信息。



图 9-62 “划分子网”对话框

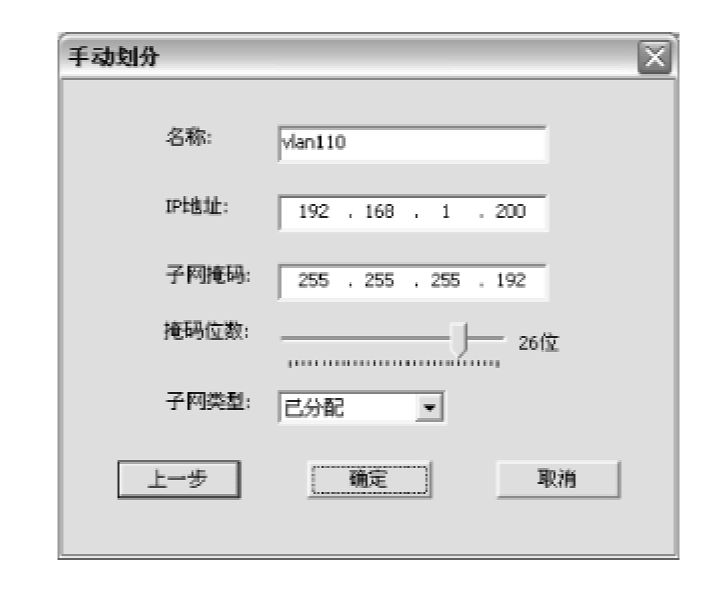


图 9-63 “手动划分”对话框

(3) 单击“确定”按钮，系统会根据要求生成指定的子网，如图 9-64 所示。

5. IP 地址扫描

使用 IP 地址扫描功能，可以扫描某一管理网段的所有 IP 地址，以及正在使用的客户端的信息，例如主机名、MAC 地址等。

在 IPMaster 主窗口右侧，右击已分配类型的节点，在快捷菜单中选择“扫描”命令，即可自动扫描已分配类型子网中所有的主机的名称、MAC 地址和使用人等，如图 9-65 所示。

6. IP 监控

使用 IP 监控功能，可以监控客户端计算机是否正常运行，以及响应时间等。

(1) 在 IPMaster 主窗口中，选中欲监控主机的“监控”复选框，如图 9-66 所示。



图 9-64　手工划分的子网



图 9-65　扫描结果



图 9-66　选定监控主机

（2）依次选择“工具”→“监控”命令，显示图 9-67 所示的“监控”对话框。在该对话框中，显示了被监控主机的运行情况。

注意：当主机关闭时，系统下方的提示信息窗口会以红色提示信息进行告警，告警记录会自动保存在可执行程序所在目录中的“告警记录.log”文件中。

用户还可以根据自己的要求，设置监控的时间间隔，在“监控间隔”文本区域中输入欲设置的时间间隔，其时间单位为“分钟”。

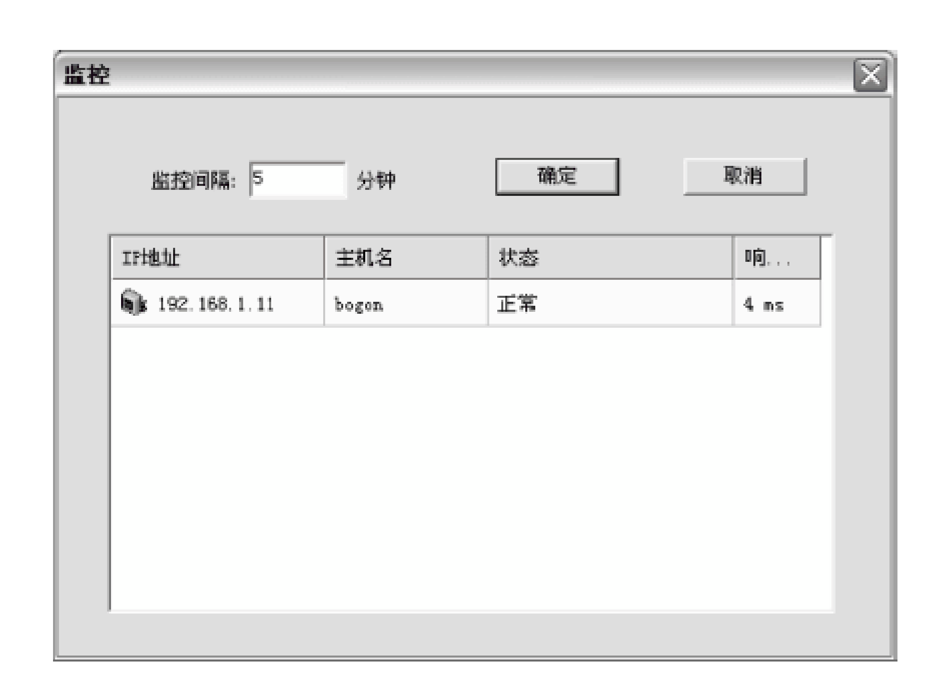


图 9-67 监控主机

9.4 共享资源管理

网络的最大特点和最主要应用是共享资源，因此，网络中共享资源的设置与应用在网络应用中占有很重要的地位。共享文件夹的权限与 NTFS 权限略有不同，NTFS 权限是针对本地用户账户和组设定的，而共享权限则是针对网络用户设定的。毫无疑问，两者都是确保数据安全的重要手段。

9.4.1 共享文件夹的权限

共享资源提供对应用程序、数据或用户个人数据的访问。既可以直接设置共享权限，也可以使用 NTFS 文件系统上的访问控制，还可以将这些方法结合起来使用。直接设置共享权限时，易于应用和管理；借助 NTFS 权限时，可以对共享资源及其内容进行更详细的控制；结合使用时，将应用更为严格的权限，例如，如果共享权限设置为“Everyone＝读取”（默认值）并且 NTFS 权限允许用户更改共享文件，则将应用共享权限，不允许用户更改文件。

除了可以直接登录到服务器访问资源外，还可以通过共享文件夹访问网络远程共享资源。因此，除了设置 NTFS 权限外，还需要设置共享文件夹权限。在“高级共享”对话框中，单击“权限”按钮，即可显示“soft 的权限”（此处以 soft 文件夹为例）对话框，显示并设置该共享文件夹的权限，如图 9-68 所示。

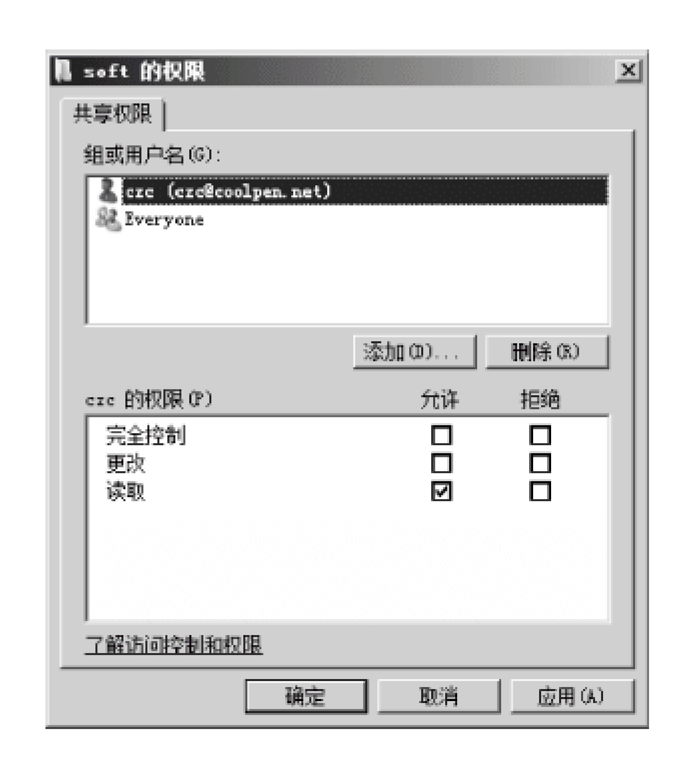


图 9-68 共享文件夹的权限

提示：通常情况下，只有在想要覆盖已指派的特定权限时，才会使用拒绝权限。另外，当创建新的共享资源时，会自动指派 Everyone 组为读取权限，这种权限是最受限制的权限。

共享文件夹权限具有以下特点。

（1）共享文件夹权限只适用于文件夹，不适用于单独的文件；只能为整个共享文件夹设置共享权限，而不能对该共享文件夹中的文件或子文件夹进行设置。所以，共享文件夹权限不如 NTFS 文件系统权限详细。

（2）共享文件夹权限并不对直接登录到计算机上的用户起作用，只适用于通过网络连接该文件夹的用户。也就是

说，共享权限对直接登录到服务器上的用户是无效的。

(3) 在FAT/FAT32系统卷上，共享文件夹权限是保证网络资源被安全访问的唯一方法。

(4) 默认的共享文件夹权限是读取，并被指定给Everyone组。

共享权限分为读取、修改和完全控制3种。不同访问权限以及对用户访问能力的控制如下。

① 读取：显示文件夹名称、文件名称、文件数据和属性，运行应用程序文件，以及改变共享文件夹内的文件夹。

② 修改：创建文件夹，向文件夹中添加文件，修改文件中的数据，向文件中追加数据，修改文件属性，删除文件夹和文件，以及执行"读取"权限所允许的操作。

③ 完全控制：修改文件权限，获得文件的所有权，执行"修改"和"读取"权限所允许的所有任务。默认情况下，Everyone组具有该权限。

共享文件夹权限的多重权限与NTFS文件系统权限相似，参考上述相关内容。在管理共享文件夹和指定共享文件夹权限时，应当注意以下几个方面的问题。

(1) 确定每个资源有哪些组需要访问，以及这些组对每个资源各自不同的权限级别。

(2) 为资源指定最严格的权限，只要允许用户完成所需要的任务即可。

(3) 在组织资源时，将对安全性要求相同的文件夹放在一个文件夹中，例如，如果用户需要拥有几个文件夹的读取权限，那么，最好将这些应用文件夹存放在同一文件夹中，然后再共享这个文件夹，而不是单独地共享每个文件夹。

(4) 使用直观的共享名，便于用户识别并找到所需要的资源。

(5) 把权限指派给组而不是用户账户，既可简化对访问权限的管理难度，又可避免权限分配出现问题。把权限指派给组易于管理共享资源，因为不用重新指派权限，只需将用户从组中添加或删除即可。若欲拒绝对共享资源的所有访问，则拒绝完全控制权限即可。

(6) 指派最具限制的权限，该权限仍允许用户执行需要的任务，例如，如果用户仅需读取文件夹中的信息并且从不删除、创建或更改文件，应当指派"读取"权限。

(7) 如果用户通过网络远程登录主机访问共享资源(如终端服务器、远程桌面等)，则用NTFS文件系统权限或访问控制设置权限即可。

(8) 共享权限只适合通过网络访问共享资源的用户，并不适用于本机登录的用户。可以和NTFS权限、访问控制等措施同时使用。

(9) 组织资源使安全性要求相同的对象定位于同一个文件夹中，例如，如果用户需要几个应用程序文件夹的"读取"权限，可将应用程序文件夹存储在同一个父文件夹中，然后，共享该父文件夹，而不是共享每个应用程序文件夹。需要注意的是，如果需要更改应用程序的位置，可能需要重新安装。

(10) 当共享应用程序时，将全部共享的应用程序组织在一个文件夹中。

(11) 将全部的应用程序组织在一个共享文件夹中可简化管理，因为这样仅有一个用来安装和升级软件的位置。

(12) 为了避免在访问网络资源时可能会出现的问题，建议不要为Everyone组设置"拒绝"权限。避免显式地给共享资源分配拒绝权限，只有在覆盖已分配的指定权限时，才有必

要显式地分配拒绝权限。

(13) Everyone 组包括任何可以访问网络资源的用户(包括 Guest 账户),但不包括 Anonymous Logon 组。

(14) 限制 Administrators 组中授予其“完全控制”权限的成员数量,从而既保证管理员能管理应用软件和控制用户权利,又不会因为拥有较高权限的用户数量太多,而导致对访问权限的滥用。

(15) 通常情况下,建议不要更改 Everyone 组的默认权限(读取),也不要擅自更改共享资源的默认位置。

(16) 尽量使用域用户账户授予用户访问权限。

(17) 已加入域的计算机,尽量通过域用户账户授权访问共享资源,而不是通过本地用户账户,从而实现对共享权限的集中管理。

(18) 使用集中数据文件夹,可以方便地管理资源和备份数据。

(19) 为共享资源使用直观的注释,确保用户和所有客户端操作系统容易识别和访问共享资源。

(20) 使用防火墙,阻止来自 Internet 的恶意访问,保护共享资源的安全。

9.4.2 共享文件夹权限与 NTFS 权限

共享文件夹权限和 NTFS 权限是可以叠加的。共享文件夹权限为资源提供有限的安全性,而 NTFS 权限为共享文件夹提供最大的灵活性。不论是在本地访问资源,还是通过网络访问该资源,NTFS 权限都是非常有用的。因此,除了设置 NTFS 权限外,还需要设置共享文件夹权限。

当管理员对 NTFS 权限和共享文件夹的权限进行组合时,组合结果所产生的权限或者是组合的 NTFS 权限,或者是组合的共享文件夹权限,哪个范围更窄、更严格就是哪一个。

例如,Folder 文件夹是 NTFS 分区上的共享文件夹。共享文件夹权限为写入;NTFS 权限为读取。网络用户最终的访问权限即为读取,而不允许写入操作,如图 9-69 所示,这样可以更加有效地确保网络安全。

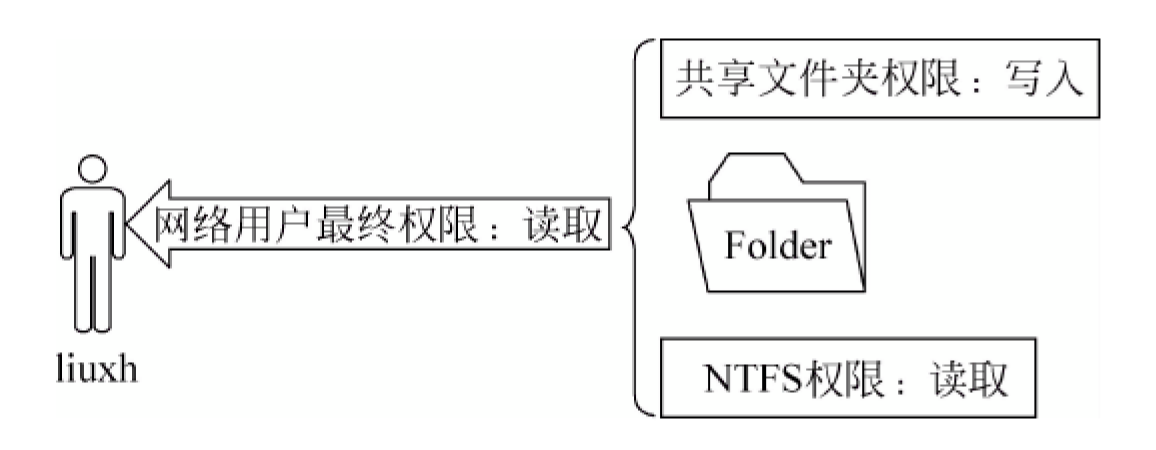


图 9-69 共享文件夹权限与 NTFS 权限叠加

当在 NTFS 卷上为共享文件夹授予共享权限时,应当遵守下述规则。

(1) 可以对共享文件夹中的文件和子文件夹应用 NTFS 权限。可以对共享文件夹中包含的每个文件和子文件夹应用不同的 NTFS 权限。

(2) 除共享文件夹权限外,用户必须要有该共享文件夹包含的文件和子文件夹的

NTFS 权限，才能访问那些文件和子文件夹。在 FAT 卷上，共享文件夹权限是保护该共享文件夹中的文件和子文件夹的唯一权限。

(3) 在 NTFS 卷上必须要求 NTFS 权限。默认情况下，Everyone 组具有"完全控制"权限。

9.4.3　设置共享文件夹

若欲实现对网络文件资源的访问，必须先将该文件夹设置为共享，然后，再赋予用户以相应的访问权限。当网络用户数量较多时，创建不同的用户组，并将拥有相同访问权限的用户加入同一个用户组，这样可以减少设置用户权限的操作。设置共享文件夹可以通过不同的方式完成，下面将分别进行介绍。

1. 在文件服务器中设置资源共享

在文件服务器中设置资源共享的步骤如下。

(1) 在"服务器管理器"窗口中，在左侧依次展开"角色"→"文件服务"→"共享和存储管理"目录，或依次选择"开始"→"管理工具"→"共享和存储管理"命令，打开图 9-70 所示的"共享和存储管理"窗口，在中间窗口会显示当前系统所共享的文件夹列表。



图 9-70　共享文件夹列表

(2) 在右侧"操作"区域，单击"设置共享"链接，显示图 9-71 所示的"设置共享文件夹向导"对话框。在"位置"文本框中输入欲设置为共享的文件夹的路径，或单击"浏览"按钮，浏览欲设置为共享的文件夹的路径。用户也可以根据实际需要，新建一个共享文件夹，并将其设置为共享。在可用卷列表中，列出当前系统中可用的卷，选择相应的卷即可，如果在列表中，没有合适的卷，用户可以自己创建一个卷。

(3) 单击"下一步"按钮，显示图 9-72 所示的"NTFS 权限"对话框。指定 NTFS 权限以控制具体用户和组如何在本地访问该文件夹，网络中的用户访问该文件夹时，就会以其所登录的用户的权限来访问该文件夹。选中"否，不更改 NTFS 权限"单选按钮，将会以该文件夹自己的 NTFS 设置来控制允许访问的用户；选中"是，更改 NTFS 权限"单选按钮，并单击"编辑权限"按钮即可根据需要设置该文件夹的访问权限。

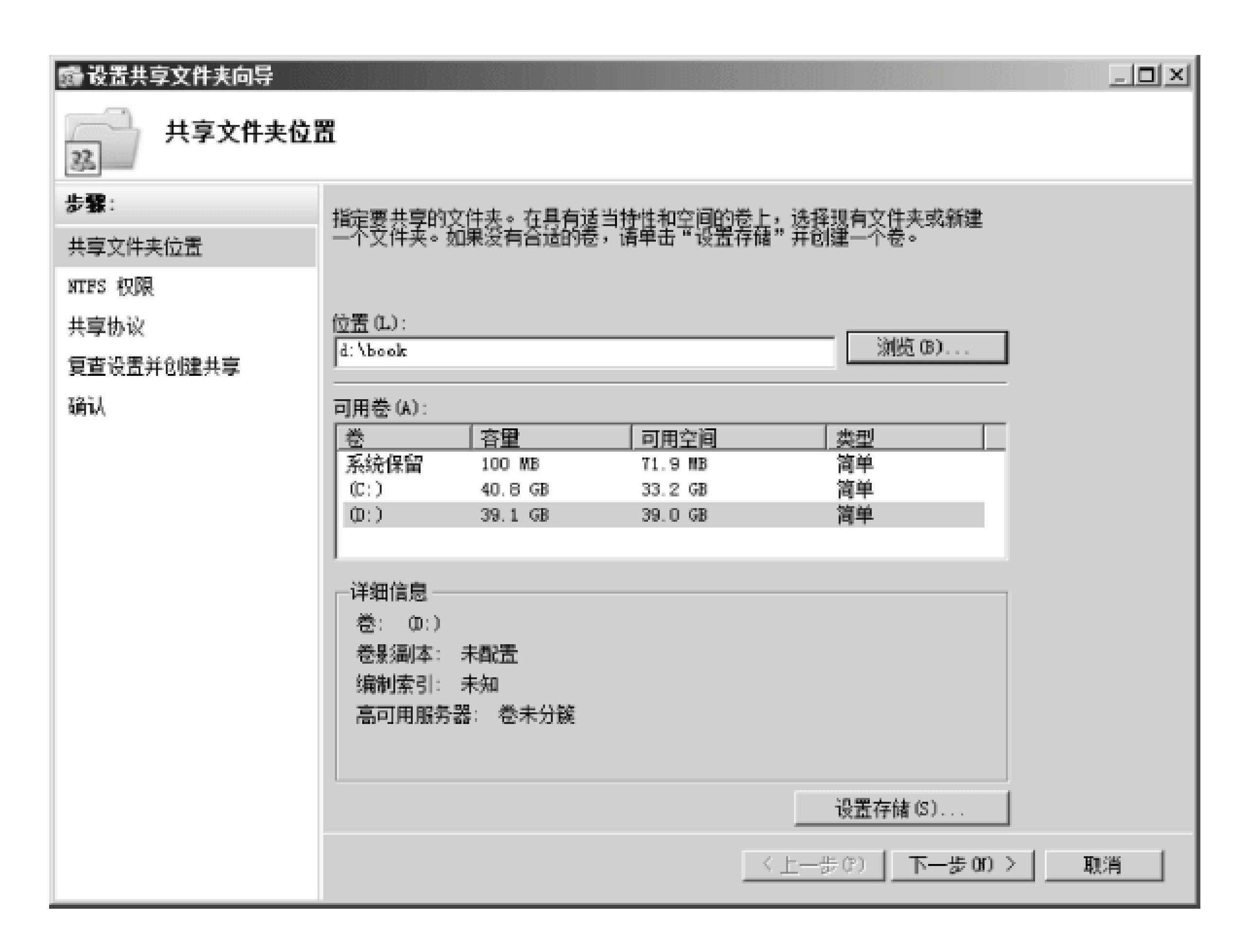


图 9-71 “设置共享文件夹向导”对话框

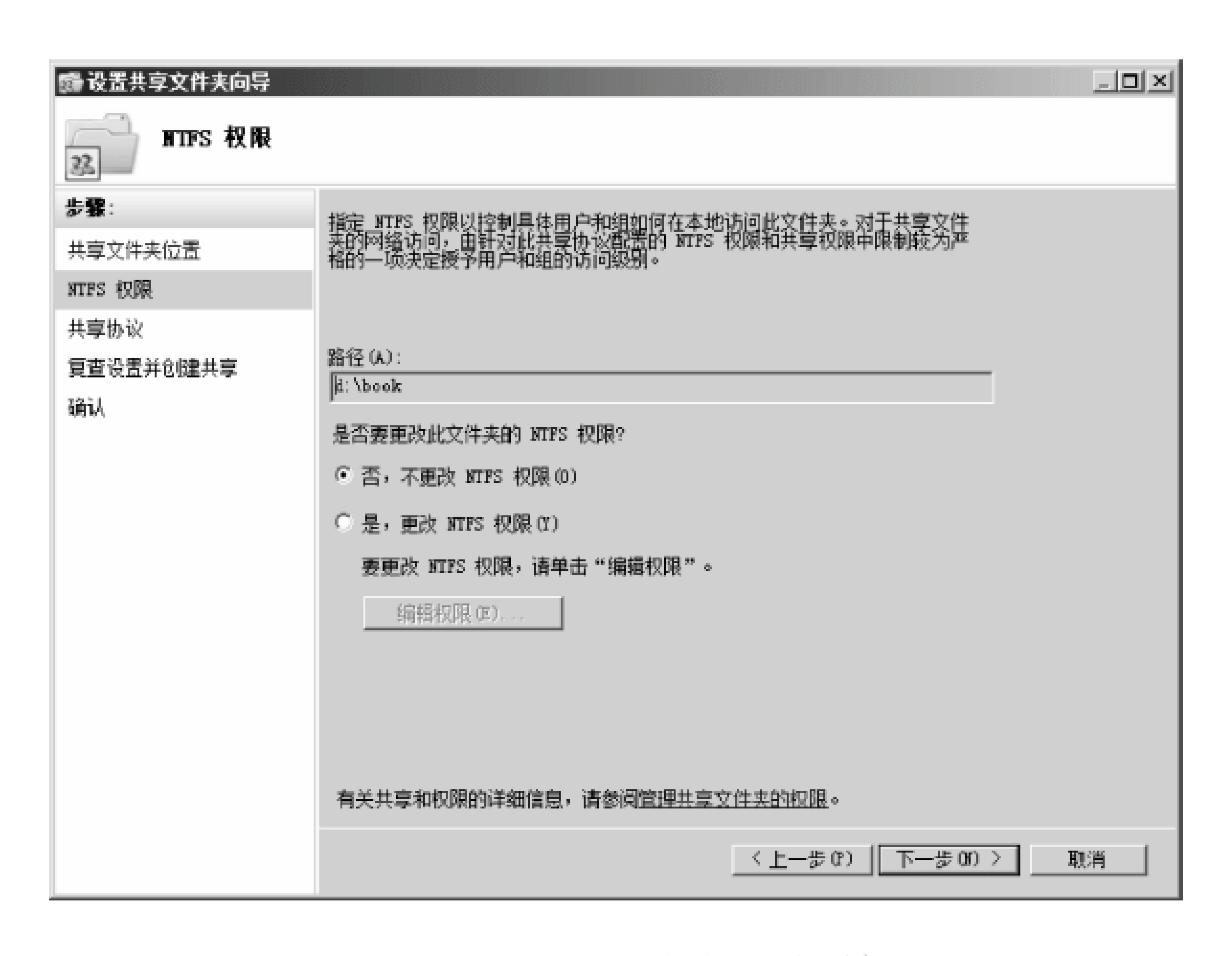


图 9-72 “NTFS 权限”对话框

(4) 单击“下一步”按钮,显示图 9-73 所示的“共享协议”对话框,根据需要选择可访问该共享文件夹的协议,因为这里没有安装分布式文件系统,因此 NFS 选项为不可用状态。选中 SMB 复选框,在“共享名”文本框中输入欲让用户看到的文件夹名称,在“共享路径”中显示的是用户访问该文件夹时所使用的网络路径。

(5) 单击“下一步”按钮,显示图 9-74 所示的“SMB 设置”对话框。指定客户端如何通过 SMB 协议访问此文件夹,用户可以在“描述”文本框中添加如何使用该共享文件夹的信息等。在“高级设置”选项区域,可以设置“用户限制”、“基于访问权限的枚举”和“脱机设置”。

(6) 单击“高级”按钮,显示图 9-75 所示的“高级”对话框。如果服务器的性能不是很好的话,可以在这里限制同时访问该服务器的用户数量,从而达到减小服务器负荷的目的。选中“允许的最多用户数量”单选按钮,并在文本框中输入欲设置的用户数量。选中“启用基于访问权限的枚举”复选框,可以根据具体用户的访问权限筛选用户可以看到的共享文件夹,从而避免显示用户无权访问的文件夹和其他共享资源。



图 9-73　“共享协议”对话框



图 9-74　“SMB 设置”对话框

（7）选择“缓存”选项卡，如图 9-76 所示。设置允许用户访问的共享内容，以及如何使用，具体设置包括如下内容。

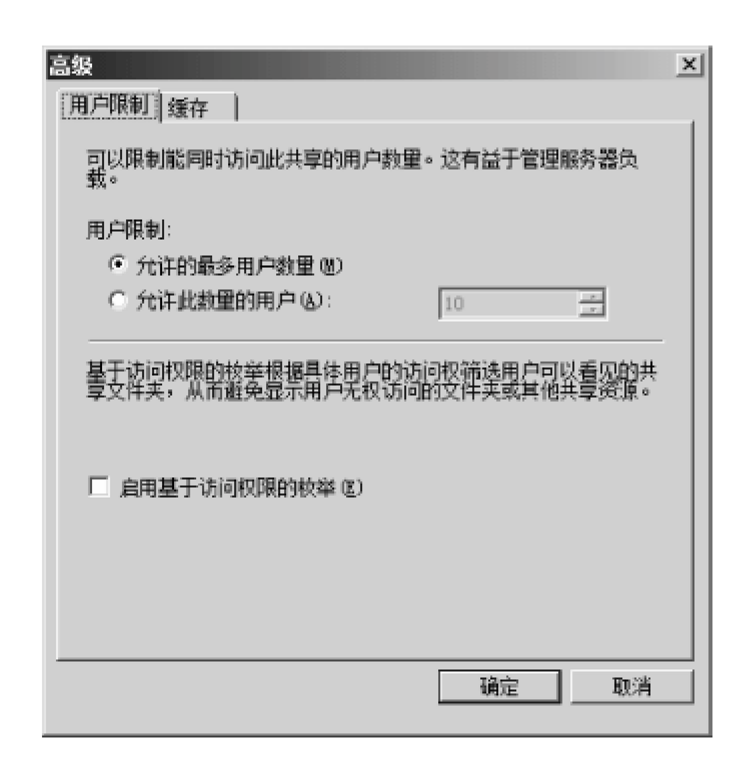


图 9-75　“高级”对话框

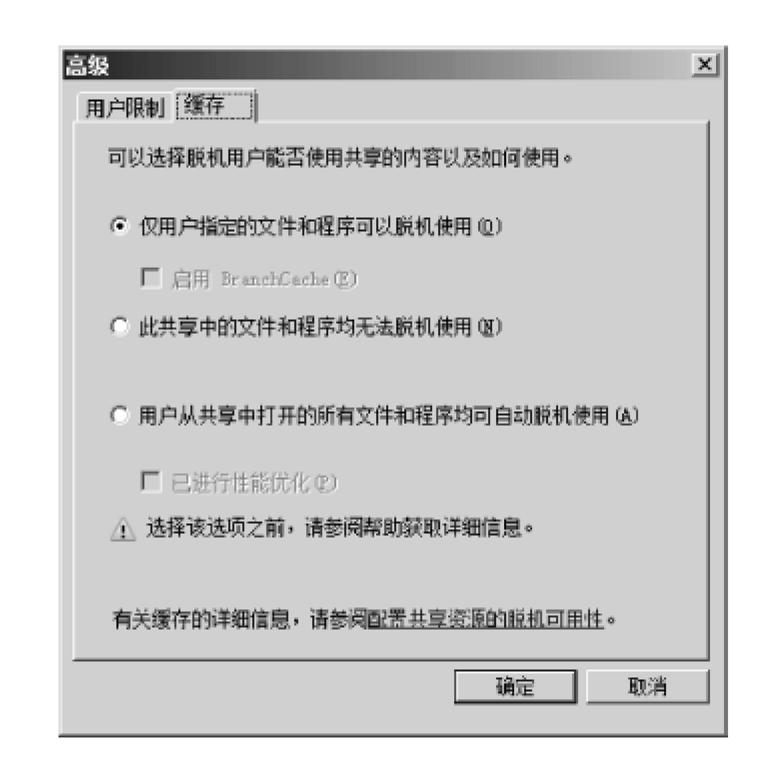


图 9-76　“缓存”选项卡

① 只允许用户访问和使用指定的文件与程序。

② 允许用户访问和使用所有共享中的文件与程序。

③ 禁止用户访问和使用共享中的所有文件与程序。

(8) 单击“确定”按钮,返回“SMB 设置”对话框,并单击“下一步”按钮,显示图 9-77 所示的“SMB 权限”对话框。在“共享路径”中所显示的即为网络中用户的访问路径,在下面的权限设置区域中,设置该共享文件夹的基本共享权限。

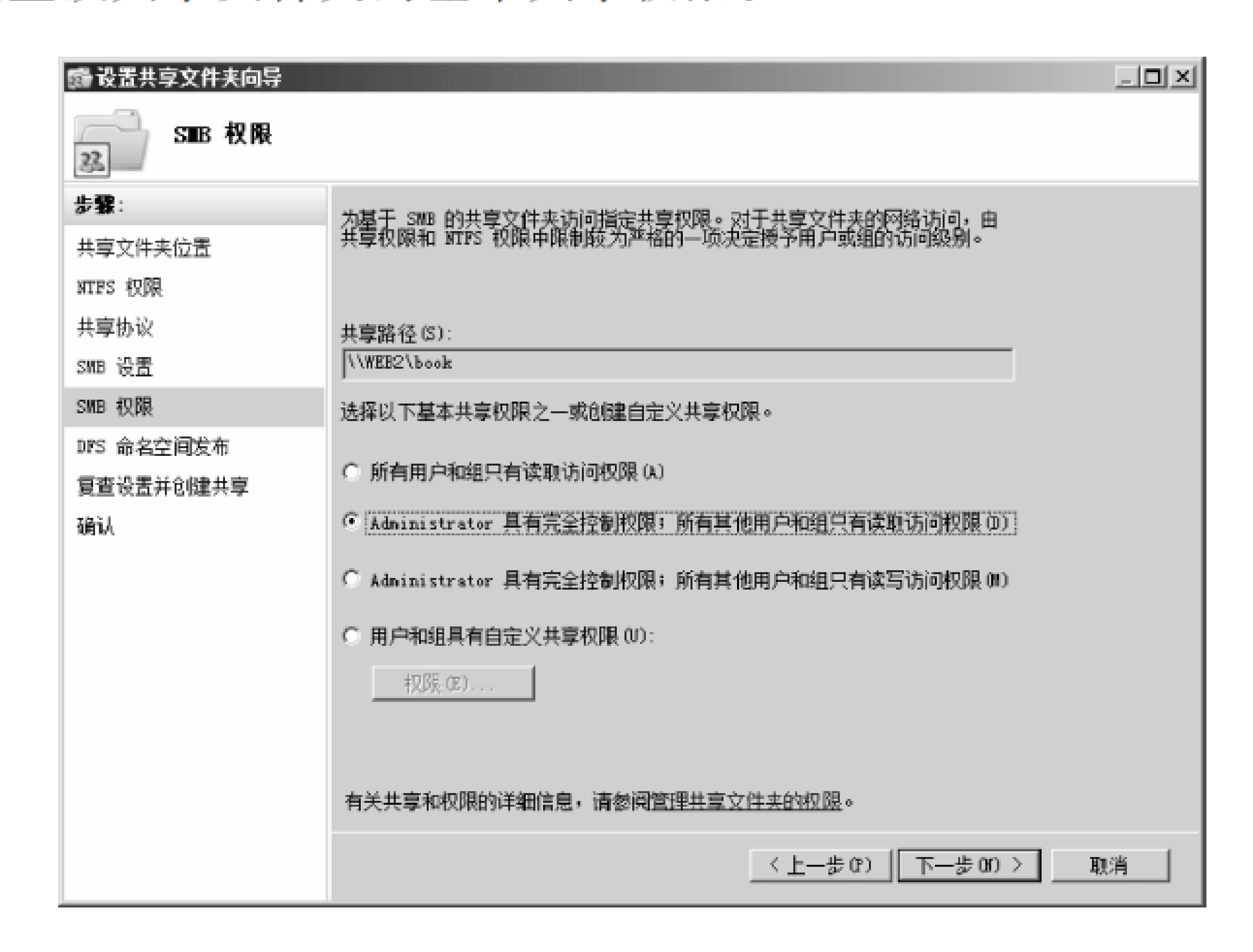


图 9-77 “SMB 设置”对话框

(9) 单击“下一步”按钮,显示图 9-78 所示的“DFS 命名空间发布”对话框。指定现有的 DFS 命名空间以及欲在该命名空间创建的文件夹,并将该共享文件夹发布到命名空间中,具体关于 DFS 命名空间的内容,可参见相关内容,这里就不再赘述。通常情况下,保持默认设置即可。



图 9-78 “DFS 命名空间发布”对话框

(10) 单击“下一步”按钮,显示图 9-79 所示的“复查设置并创建共享”对话框。在“共享文件夹设置”中检查前面所做的设置是否正确,单击“上一步”按钮,可返回重新设置。



图 9-79 “复查设置并创建共享”对话框

（11）单击“创建”按钮，系统开始进行创建操作，创建成功后，显示图 9-80 所示的“确认”对话框。单击“关闭”按钮，完成在文件服务器中设置共享的操作。此时新创建的共享即可显示在“服务器管理器”窗口中。



图 9-80 “确认”对话框

2. 在资源管理器中设置

与在文件服务器中设置共享相比，在资源管理器中设置共享要简单得多。具体的操作步骤如下。

（1）打开 Windows 资源管理器，选择想要设置共享或者已经创建共享的文件夹或驱动器，右击并选择快捷菜单中的“共享”命令，打开“文件共享”对话框。在用户下拉列表框中选择欲设置允许访问该共享的用户，单击“添加”按钮将该用户添加到正下方的用户列表中。

（2）添加用户完成后，在用户列表中，单击欲设置权限的用户名的“权限级别”下拉列表框，并在列表中选择该用户的访问权限：“读取”、“所有者”和“写入”，如图 9-81 所示。

（3）设置完成后，单击“共享”按钮，确认共享该文件夹，显示图 9-82 所示的“您的文件

夹已共享”对话框，单击“完成”按钮完成共享。




图 9-81 设置用户访问权限



图 9-82 完成共享

3. 在控制台树中设置

（1）依次选择“开始”→“管理工具”→“计算机管理”命令，打开“计算机管理”控制台，接着在左侧栏目录树中，展开“共享文件夹”目录树并选择“共享”选项，显示图 9-83 所示的窗口。“共享文件夹”选项提供有关本地计算机上的所有“共享”、“会话”和“打开文件”的相关信息，可以查看本地计算机和远程计算机的连接与资源使用概况。

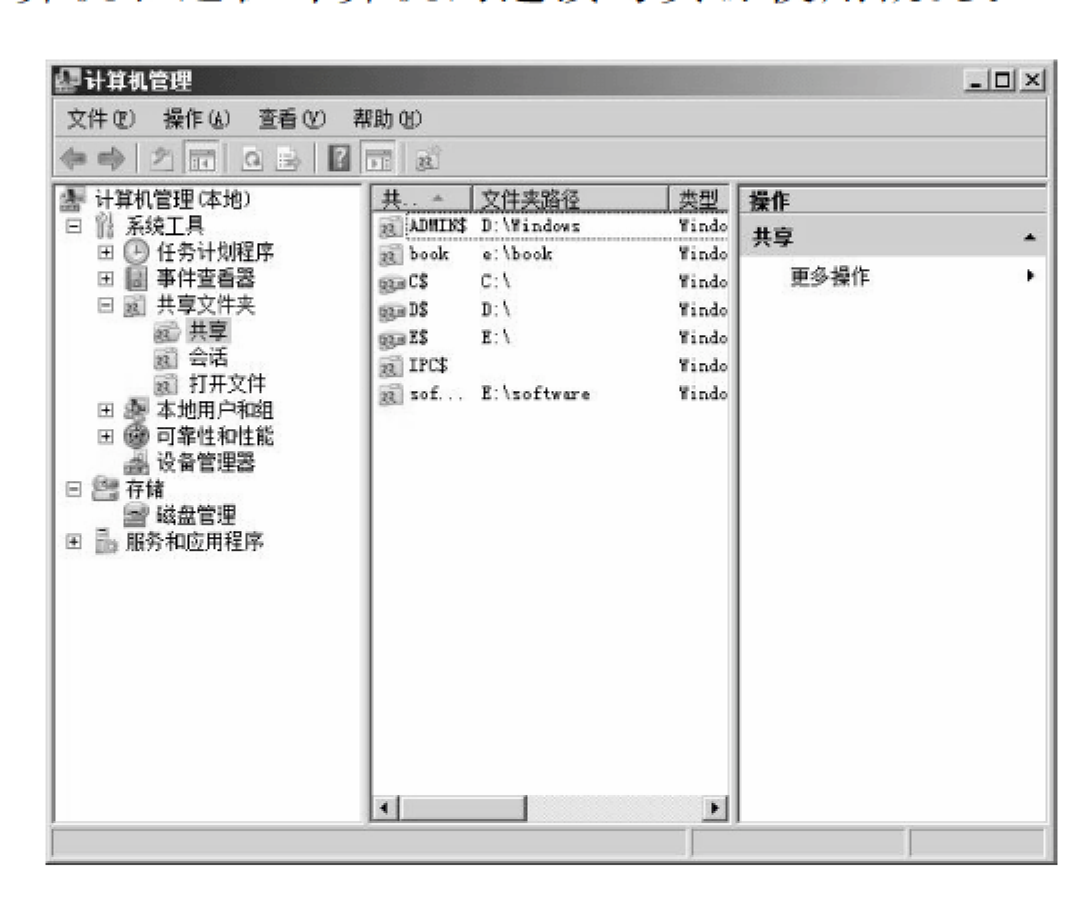


图 9-83 “计算机管理”窗口

（2）右击“共享”选项，在快捷菜单中选择“新建共享”命令，即可打开“创建共享文件夹向导”对话框。

（3）单击“下一步”按钮，显示图 9-84 所示的“文件夹路径”对话框。在“文件夹路径”文本框中输入欲设置为共享的文件夹路径，或单击“浏览”按钮选择文件夹或创建新的文件夹。

（4）单击“下一步”按钮，显示图 9-85 所示的“名称、描述和设置”对话框，指定用户如何在网络上查看和使用该共享。在“共享名”文本框中，输入显示在网络上的共享名称；“共享路径”中所显示的即为网络访问路径；在“描述”文本框中，添加该共享的描述信息。单击“更改”按钮，可以修改该共享的“脱机设置”。



图 9-84　“文件夹路径”对话框

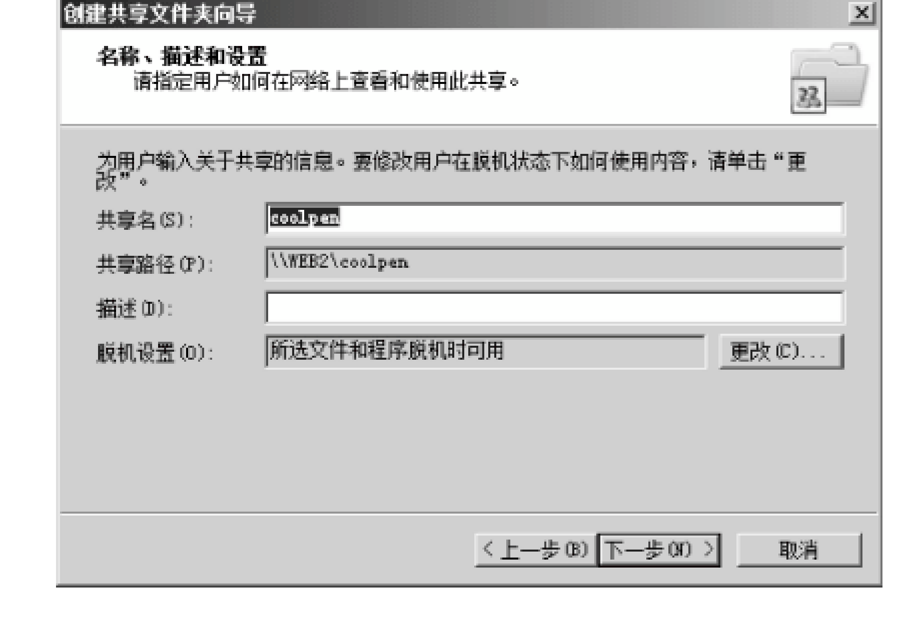


图 9-85　“名称、描述和设置”对话框

(5) 单击“下一步”按钮，显示图 9-86 所示的“共享文件夹的权限”对话框。通过设置权限，能够控制可以查看该共享的用户及其访问级别。

(6) 单击“完成”按钮，系统即可开始执行共享操作。最后，显示图 9-87 所示的“共享成功”对话框，单击“完成”按钮，完成该共享内容的操作。如果选中“当单击‘完成’时，再次运行该向导来共享另一个文件夹”复选框，将会在单击“完成”按钮后，再次运行新建共享向导。

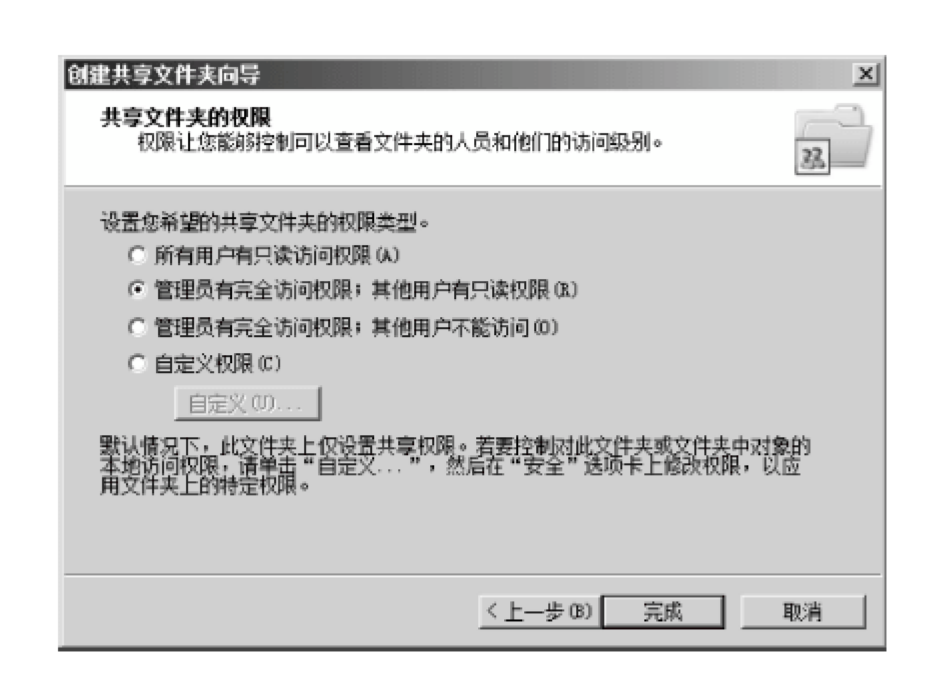


图 9-86　“共享文件夹的权限”对话框

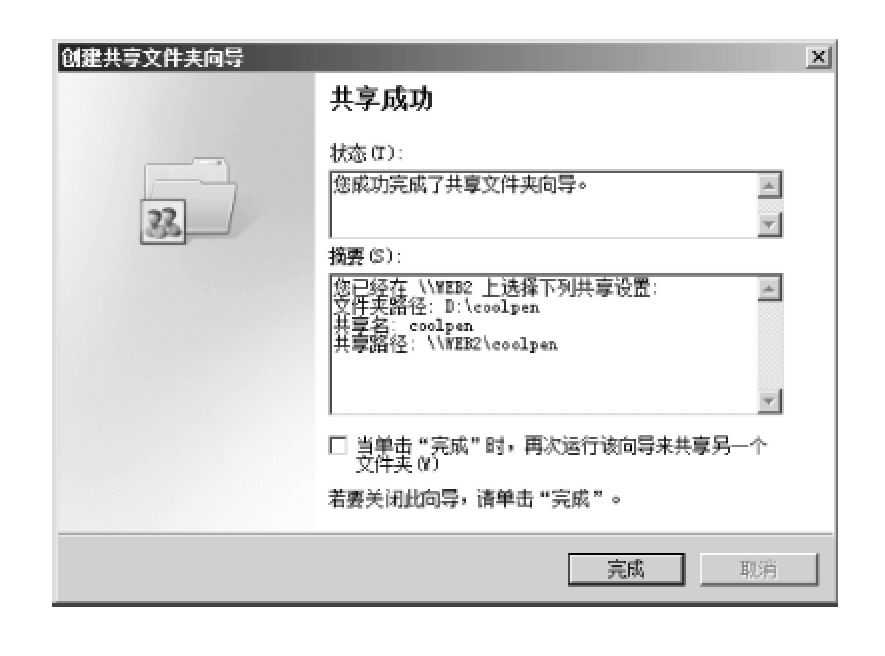


图 9-87　“共享成功”对话框

9.4.4　访问共享文件夹资源

企业网络中的客户端计算机，可以采用多种方式实现对文件服务器的访问。不同共享文件夹的访问方式各有其特点，可以根据实际需要选择。下面以 Windows Vista 客户端系统为例进行介绍。

1. 网络

依次选择“开始”→“网络”命令，打开图 9-88 所示的“网络”窗口，系统会自动发现网络中的计算机。双击想要访问共享的计算机，在弹出的窗口中，输入具有访问权限的用户名和密码即可。

2. Windows 资源管理器

打开 Windows 资源管理器，在“地址”栏中输入“\\计算机名\共享名”或“\\计算机 IP



图 9-88 “网络”窗口

地址\共享名”，即可实现对文件服务器中相应共享文件夹的访问，如图 9-89 所示。当然，用户必须拥有相应的访问权限才行。



图 9-89 从资源管理器中访问共享

3. 映射网络驱动器

如果需要经常访问文件服务器中的共享资源，可以采用映射网络驱动器的方式，将共享文件夹映射为本地计算机的一个网络驱动器。

右击欲设置为网络驱动器的共享文件夹，在快捷菜单中选择“映射网络驱动器”命令，显示“映射网络驱动器”对话框，如图 9-90 所示。在“驱动器”下拉列表框中，选择分配给该网络驱动器的盘符即可。选中“登录时重新连接”复选框，在计算机启动时会自动挂接该共享文件夹，而不必每次都执行映射操作。最后，单击“完成”按钮即可。

9.4.5 监视对共享文件夹的访问

当网络中存在多个客户端访问共享文件夹时，如果用户数量太多或有多个用户同时打开同一个文件时，则可能会因为服务器负担过重而造成死机。因此，管理员需要时刻关注共享文件的使用情况，即需要监视有哪些客户端与服务器连接，以及打开了哪些文件等。

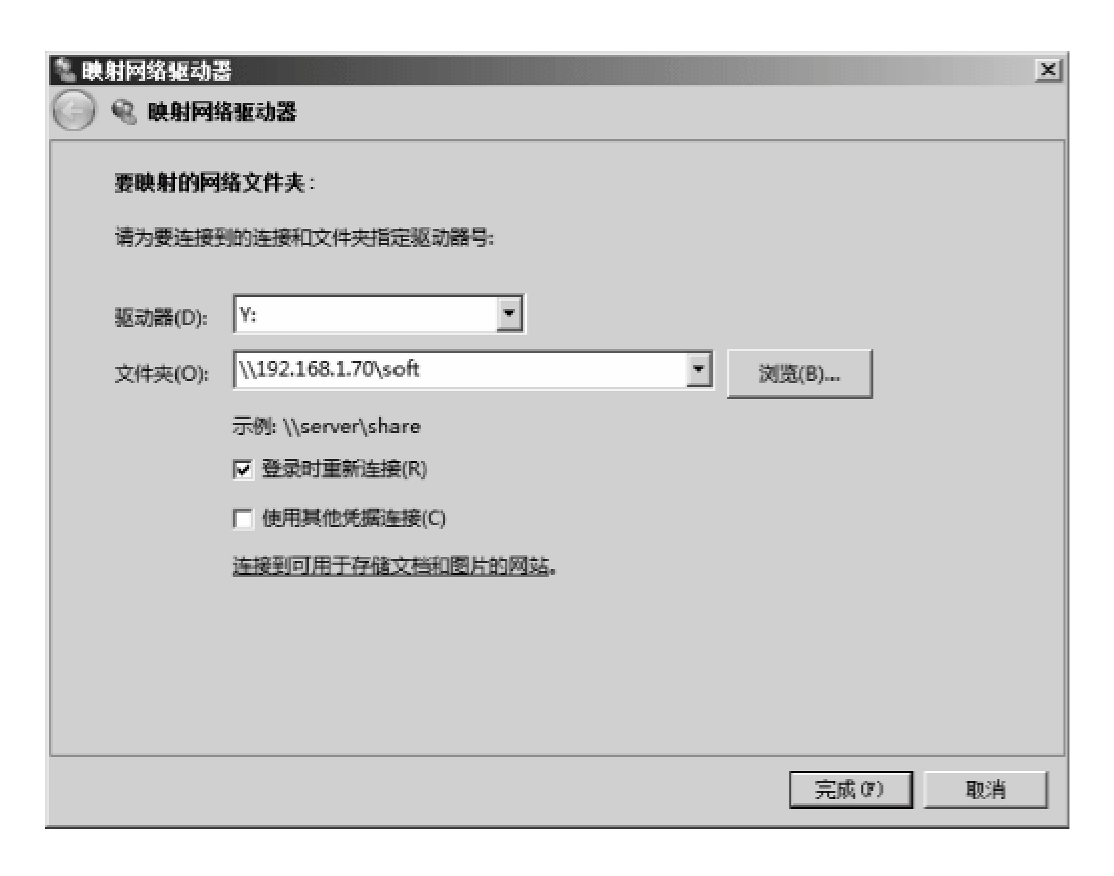


图 9-90　“映射网络驱动器”对话框

1. 监视会话

通常情况下，当客户端计算机访问文件服务器时，会自动建立一个会话连接，通过这些会话记录，管理员可以轻松查看用户所建立的会话情况。另外，当客户端计算机关闭所打开的文件后，其连接有可能仍然存在，此时，则可以手动关闭这些会话连接。

（1）在“共享和存储管理”窗口右侧的“操作”栏中，单击“管理会话”按钮，显示“管理会话”窗口。在“会话”列表中，显示了当前所有的会话信息，例如访问共享所使用的用户、计算机、打开的文件或文件夹数量、连接时间和空闲时间等，如图 9-91 所示。

（2）在“会话”列表中，选中想要关闭的会话，单击“关闭所选文件”按钮，显示图 9-92 所示的“共享和存储管理”警告框。提示如果在不发出警告的情况下断开连接，用户可能会丢失数据。

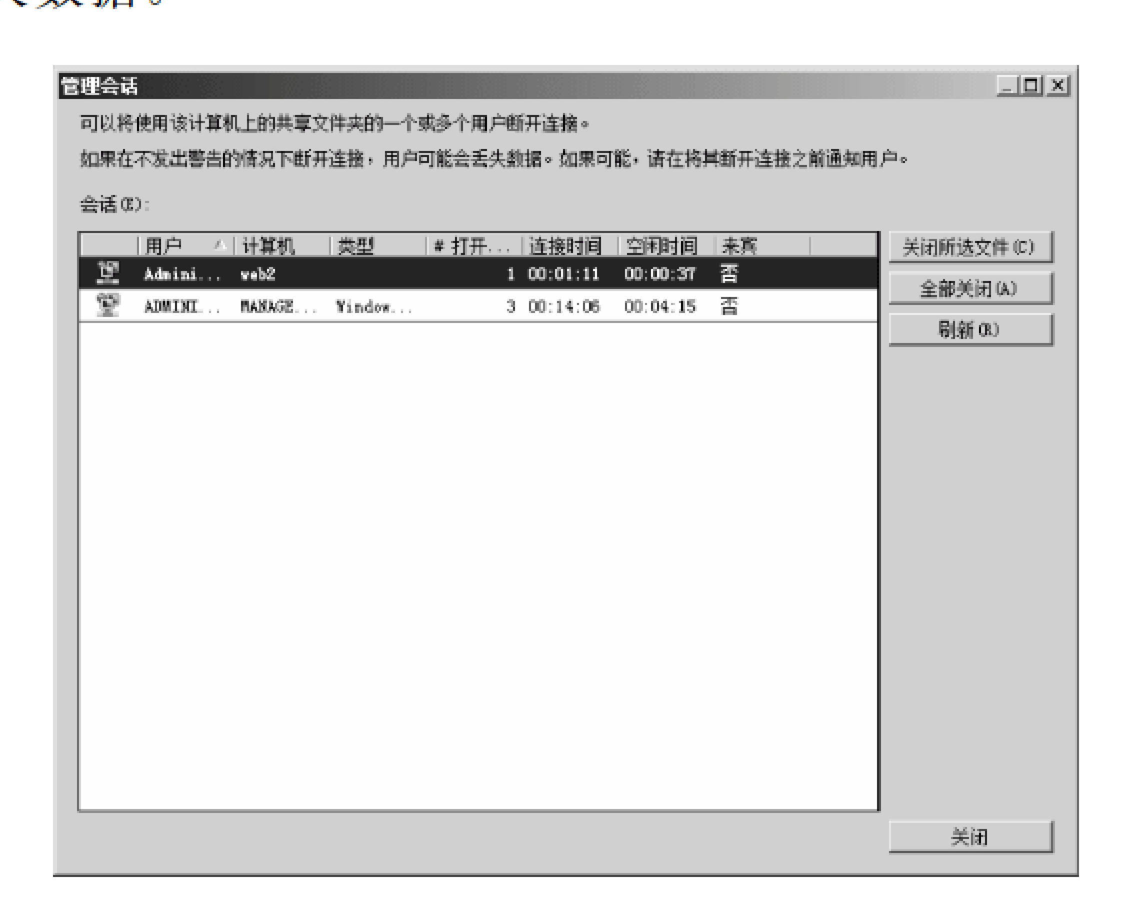



图 9-91　“管理会话”窗口

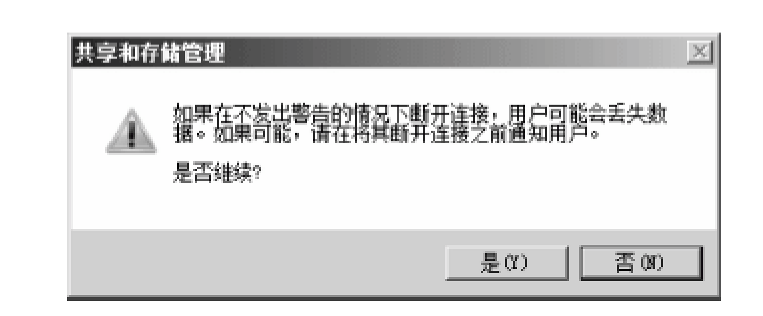


图 9-92　“共享和存储管理”警告框

（3）单击“是”按钮，可以立即断开该连接。

提示：如果存在多个共享会话，在“管理会话”对话框中，单击“全部关闭”按钮，则可断开所有会话。

另外，还可以在“计算机管理”窗口中，查看会话连接，依次展开“计算机管理(本地)”→

“系统工具”→“共享文件夹”→“会话”目录，在中间窗口中即可查看当前所建立的会话连接，如图 9-93 所示。同样右击会话连接，在快捷菜单中选择“关闭会话”命令，即可断开所选的连接。



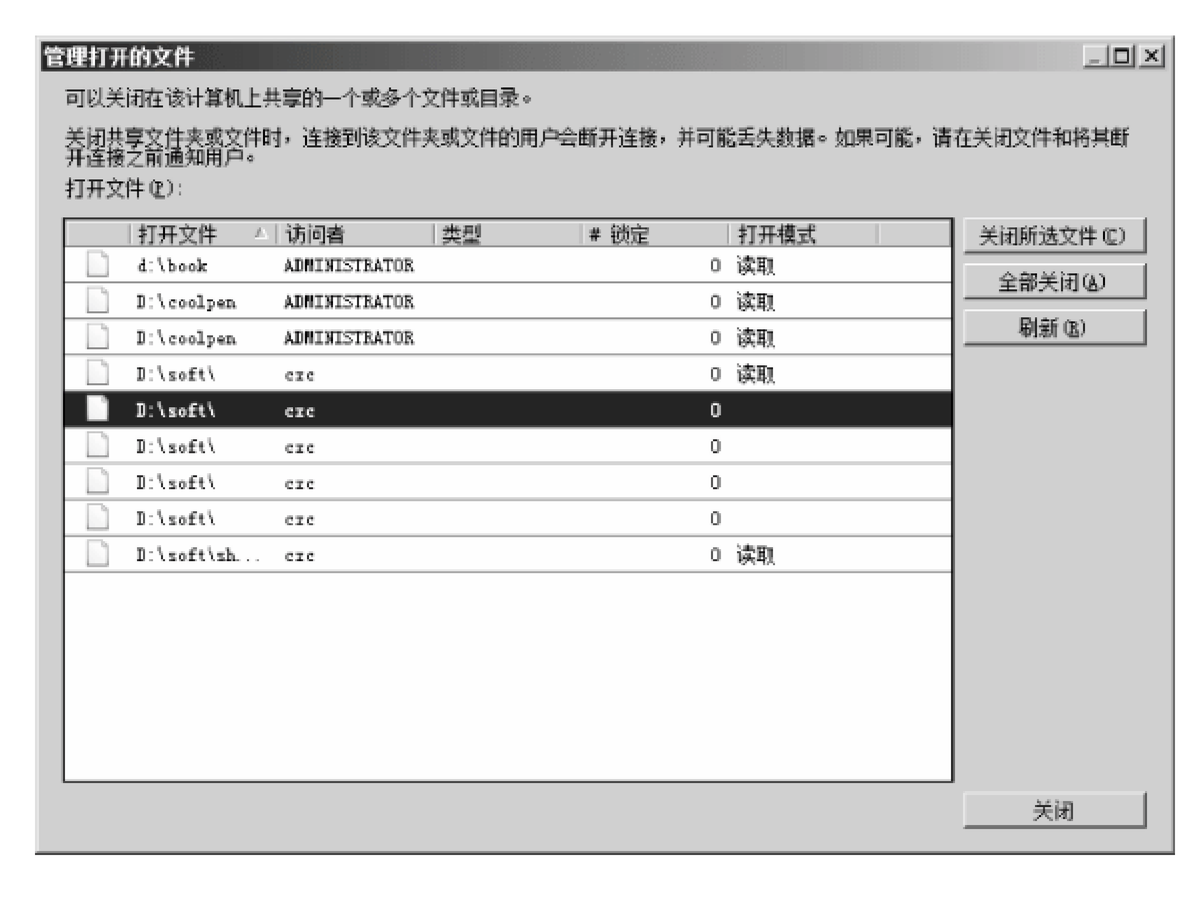
图 9-93 查看会话连接

2. 监视打开的文件

通过查看用户所打开的文件，可以详细了解当前共享的使用情况，还可以及时阻止一些非常规使用情况的发生。

(1) 在“共享和存储管理”窗口中，在右侧“操作”栏中，单击“管理打开的文件”按钮，显示“管理打开的文件”窗口。在“打开文件”列表中，详细显示了当前用户所访问的共享，以及打开的共享文件，如图 9-94 所示。

(2) 在“打开文件”列表中，选中想要关闭用户已打开的文件。单击“关闭所选文件”按钮，显示图 9-95 所示的“共享和存储管理”警告框。提示如果在不发出警告的情况下断开连接，用户可能会丢失数据。





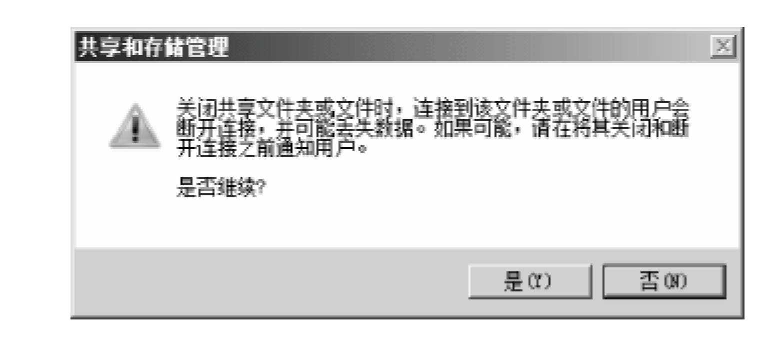


图 9-94 “管理打开的文件”窗口　　图 9-95 “共享和存储管理”警告框

(3) 单击“是”按钮，可以立即断开该连接。

另外，还可以在“计算机管理”窗口中，查看远程用户所打开的文件，依次展开“计算机管

理”→“系统工具”→“共享文件夹”→“打开文件”目录，在中间窗口中即可查看所有已打开的文件，如图 9-96 所示。右击会话连接，在快捷菜单中选择“将打开的文件关闭”命令即可。



图 9-96　关闭打开的文件

9.5　域用户管理

网络上的每个使用者都是用户，而用户在网络中的权利则是由其对应的用户账户决定的。用户的权限不同，对计算机及网络控制的能力与范围就不同。组是网络管理中最常用的目录对象之一，管理员可以将希望统一管理的对象添加到相同的组中，然后对组进行管理和设置，并自动将这些设置传播给其成员，例如用户组、计算机组等。

9.5.1　用户账户的管理

用户账户的管理是网络管理员的一项重要任务，主要包括创建用户账户、设置登录属性、禁用账户、删除账户、限制用户登录行为等。看似简单的操作，稍有不慎很可能导致安全漏洞的产生。灵活掌握各项管理任务的操作，可以使管理员的工作事半功倍。

1. 创建用户账户

通常情况下，只有域管理员或者被委派创建用户账户权限的用户才可以创建用户账户。默认情况下，域控制器已经启用了对用户账户密码安全的一些限制，包括禁止使用简单密码、空白密码、使用期限等。

（1）在“服务器管理器”窗口中，展开指定域控制器下的“Active Directory 用户和计算机”目录，选择 Users 选项，显示图 9-97 所示的窗口，列出了系统默认用户账户。

（2）在右侧窗口空白处右击，选择快捷菜单中的“新建”→“用户”命令，打开图 9-98 所示的“新建对象 - 用户”对话框，输入新创建的用户的信息。在“姓”文本框中输入新用户的姓氏；在“名”文本框中输入新用户的名称；在“用户登录名”文本框中输入用户用来登录域的账号名；“用户登录名(Windows 2000 以前版本)”是用户从 Windows 2000 以前的 Windows 系统登录域时使用的用户名，保持默认即可。

提示：建议管理员在创建用户账户时，尽量输入详细的用户信息，便于日后维护和安全



图 9-97 “Active Directory 用户和计算机”窗口

管理工作。

(3) 单击“下一步”按钮，显示图 9-99 所示的对话框，为新添加的用户指定登录域时使用的密码，并指定对于密码的控制权限。操作方法与本地计算机上创建用户账户时完全相同，此处不再赘述。



图 9-98 “新建对象 - 用户”对话框



图 9-99 设置用户账户密码

提示：为了提高网络的安全性，对所有账户密码的设置，应尽量使用含字母、数字及下划线随机组合的密码，密码之间尽量不相关，以确保账户的安全。

(4) 单击“下一步”按钮，显示图 9-100 所示的用户信息摘要对话框，单击“完成”按钮，即可完成新用户的创建。

注意：如果设置的密码不符合 Windows Server 2008 网络系统密码规则，将提示图 9-101 所示的“Active Directory 域服务”对话框，返回重新更改即可。



图 9-100 确认新用户信息

2. 设置用户账户属性

活动目录的一个基本特点就是目录管理功能，对于用户账户的管理而言，管理员可以通过用户账户检索到对应用户的大量实用信息，包括 E-mail 地址、手机、家庭电话、办公室电话等基本信息，以及其他网络管理信息，例如配置文件设置、访问权限、所属组等。为了确保用户信息的时效性，管理员创建账户时应尽量完善相关信息，并及时更新。下面以 liuxh 用户账户为例，分别介绍主要选项卡中的用户账户属性设置。

（1）“常规”选项卡

在“常规”选项卡中，可以设置用户的常用信息，如图 9-102 所示。主要包括“姓”、“名”、“显示名称”、“描述”、“电子邮件”、“电话号码”、“网页”等基本信息。

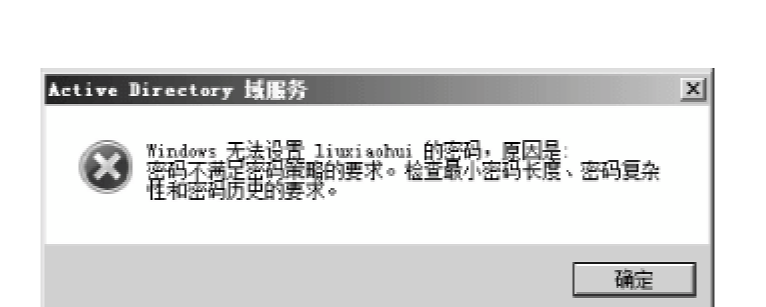


图 9-101　“Active Directory 域服务”对话框

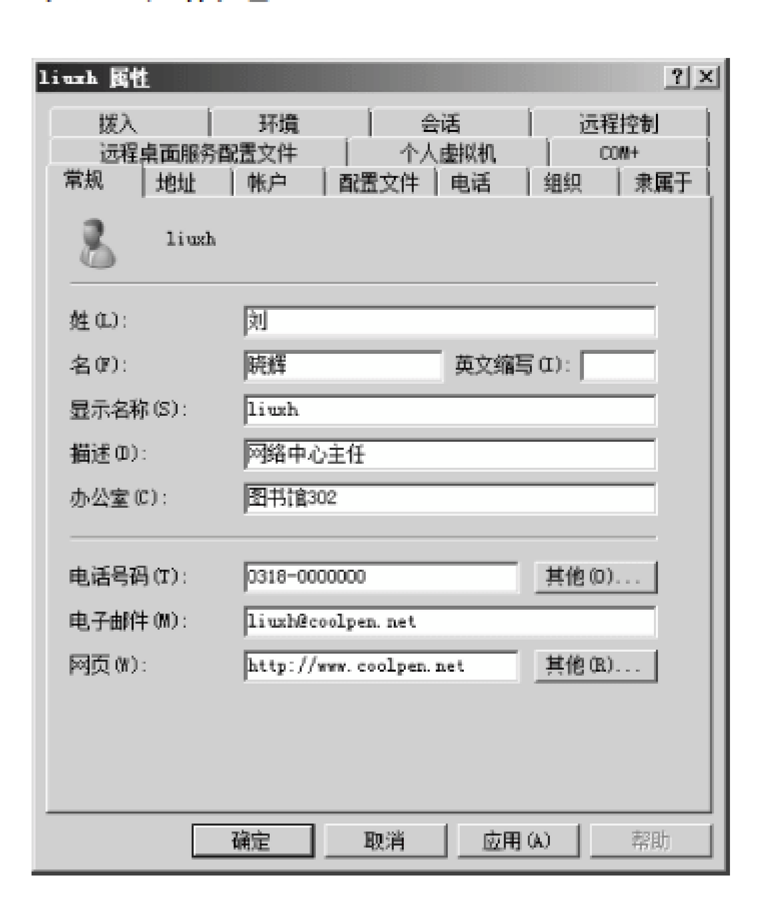


图 9-102　“常规”选项卡

（2）“地址”选项卡

在“地址”选项卡中可以设置用户所属的“国家/地区”、“省/自治区”、“市/县”、“街道”、“邮政信箱”和“邮政编码”等通信地址信息，如图 9-103 所示。

（3）“账户”选项卡

在“账户”选项卡中可以对用户的登录属性进行配置，如图 9-104 所示。

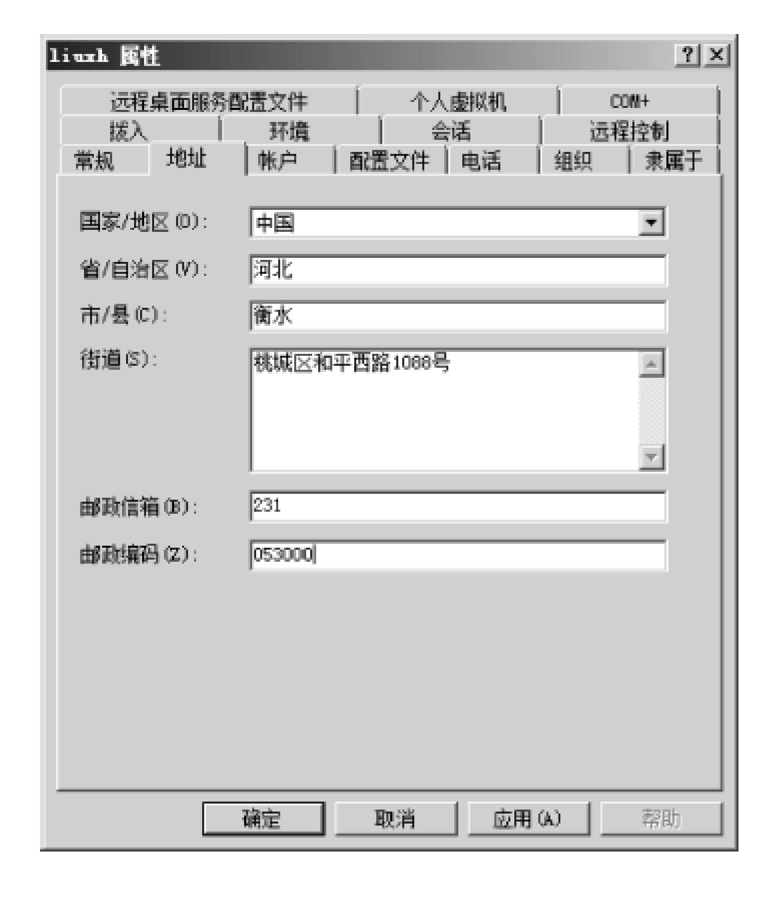


图 9-103　“地址”选项卡

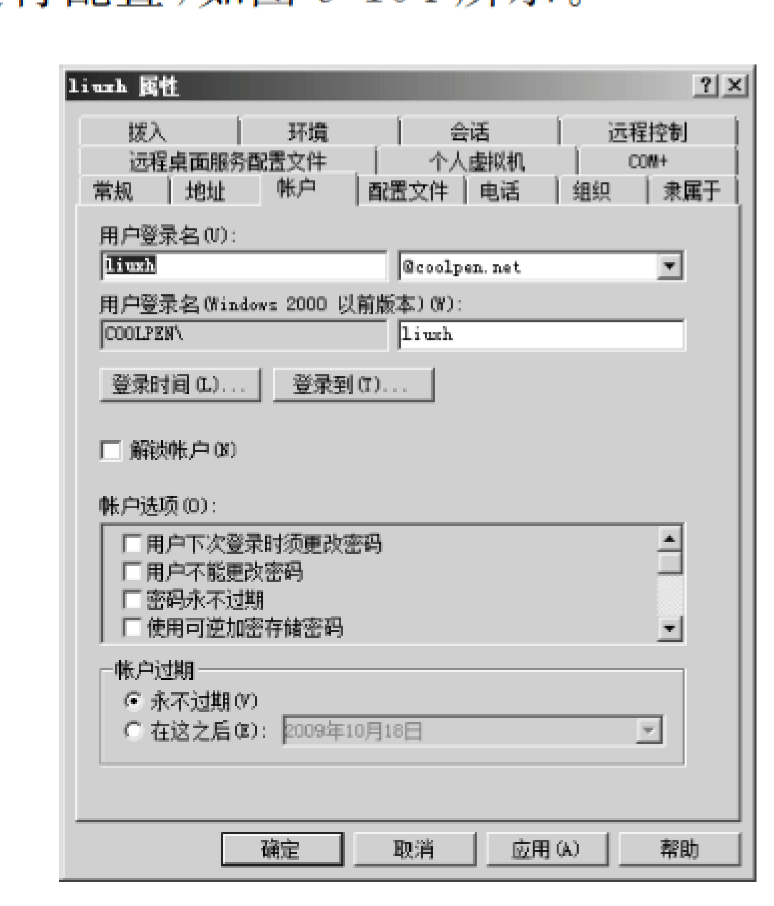


图 9-104　“账户”选项卡

如果需要修改用户的登录名,则在"用户登录名"文本框中,修改当前用户的登录名称。如果目前的环境是多域控制器并存,则可以在右侧的下拉列表框中选择其他的域名称。

注意: 如果更新了用户登录名称,则同步更新"用户登录名(Windows 2000 版本)"文本框的登录名称。

每个用户账户包含多个账户选项,这些选项能够确定如何在网上对持有特殊用户账户进行登录的人员实施身份验证。在"账户选项"列表中,可以进行当前用户账户的密码、委派等功能设置。每个选项的含义如表 9-1 所示。

表 9-1 账户选项及含义

账户选项	含义
用户下次登录时须更改密码	强制用户下次登录网络时更改密码。当希望该用户成为唯一知道其密码的人时,使用该选项
用户不能更改密码	阻止用户更改其密码。当希望保留对用户账户(如来宾或临时账户)的控制权时,使用该选项
密码永不过期	防止用户密码过期。建议"服务"账户启用该选项,并且应使用强密码
使用可逆加密存储密码	允许用户从 Apple 计算机登录 Windows 网络。如果用户不是从 Apple 计算机登录,则不应使用该选项
账户已禁用	防止用户使用选定的账户登录。许多管理员将禁用的账户用作公用用户账户的模板
交互式登录必须使用智能卡	要求用户拥有智能卡来交互地登录网络。用户还必须具有连接到其计算机的智能卡读取器以及智能卡的有效个人标识号(PIN)。当选择该选项时,用户账户的密码将被自动设置为随机且复杂的值,并设置"密码永不过期"选项
信任账户作为委派	允许在该账户下运行的服务代表网络中的其他用户账户执行操作。对于运行在受信任委派的用户账户(也称为服务账户)下的服务,可以模拟客户端以获取运行该服务的计算机或其他计算机上的资源的访问权。在设置为 Windows Server 2003 功能级别的林中,该设置位于"委派"选项卡上,且仅对已被指派了服务主体名称(SPN)(在 Windows 支持工具中使用 setspn 命令设置)的账户可用。这是一个安全敏感的功能,应当谨慎指派 该选项仅可用于运行 Windows Server 2003 的域控制器(其中域功能被设置为 Windows 2000 混合模式或 Windows 2000 纯模式)。在运行 Windows Server 2003 的域控制器上(其中域功能级别被设置为 Windows Server 2003),使用"委派"选项卡来配置委派设置。仅对具有已指派 SPN 的账户,才显示"委派"选项卡
敏感账户,不能被委派	允许对用户账户进行控制,例如来宾账户或临时账户。如果该账户不能被其他用户账户指派为委派,就可以使用该选项
此账户需要使用 DES 加密类型	提供对数据加密标准(DES)的支持。DES 支持多级加密,包括 MPPE 标准(40 位)、MPPE 标准(56 位)、MPPE 强加密(128 位)、IPSecDES(40 位)、IPSec56 位 DES 以及 IPSec 三级 DES(3DES)
不要求 Kerberos 预身份验证	支持 Kerberos 协议的备用实现。运行 Windows 2000 或 Windows Server 2003 的域控制器,可使用其他机制来同步时间。由于预身份验证提供了附加安全性,因此在启用该选项的时候要小心

(4)"配置文件"选项卡

在"配置文件"选项卡中,可以设置用户的"配置文件路径"和"主文件夹"路径,如图 9-105 所示。主文件夹也称为主目录,是分配给用户用于私人用途的文件夹。虽然应用程序有自己默认的文件夹存储和打开文件,但是主文件夹将是命令行下用户的默认工作文件夹。可

以为用户的主文件夹指定本地路径，但是仅有当用户在本地登录的时候才生效。对于从网络登录的用户，需要选中“连接”单选按钮，并使用遵守 UNC 规则的网络路径，文件夹名称支持用户变量的模式，如%Username%。

当为用户指定主文件夹的时候，如果网络共享已经存在并且对该共享具备写入的权限，服务器会自动创建该用户的主文件夹。

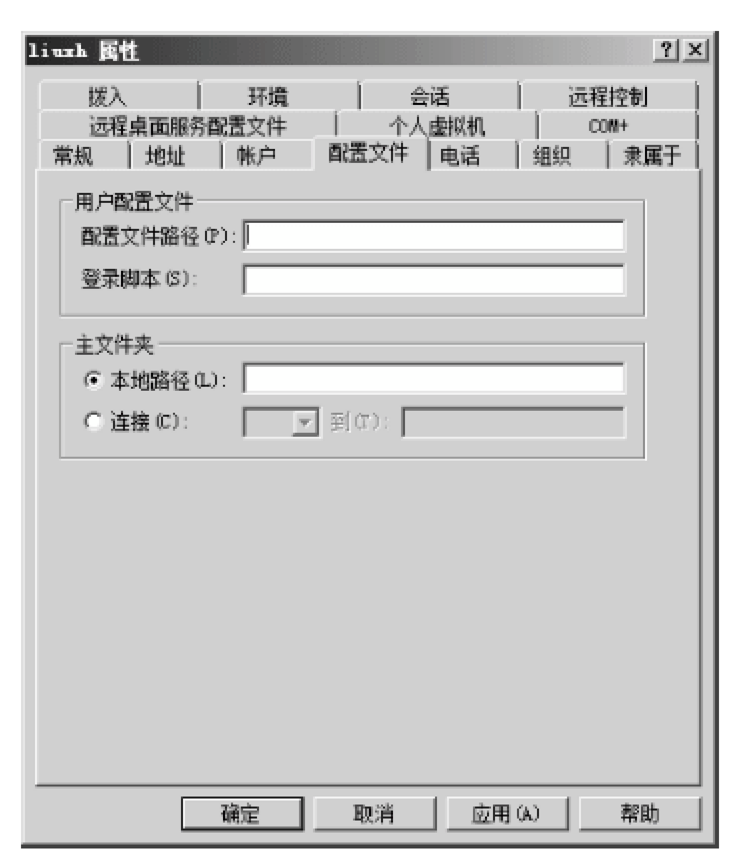


图 9-105　“配置文件”选项卡

（5）“隶属于”选项卡

在“隶属于”选项卡中，可以对用户所属的组进行设置，如图 9-106 所示。单击“添加”按钮，可以将当前用户账户添加到指定组中，同时在“隶属于”列表中显示该组名。选择组名后单击“删除”按钮，即可将账户从组中脱离。同一用户账户可以隶属于不同的组。

（6）“环境”选项卡

在“环境”选项卡中，可以设置用户登录终端的运行环境，替代任何可能已经在用户的客户登录设置中出现的相关设置，如图 9-107 所示。如果希望在登录的时候运行指定的程序，在“程序文件名”文本框中输入可执行的应用程序的文件名，在“开始位置”文本框中输入应用程序的工作目录。

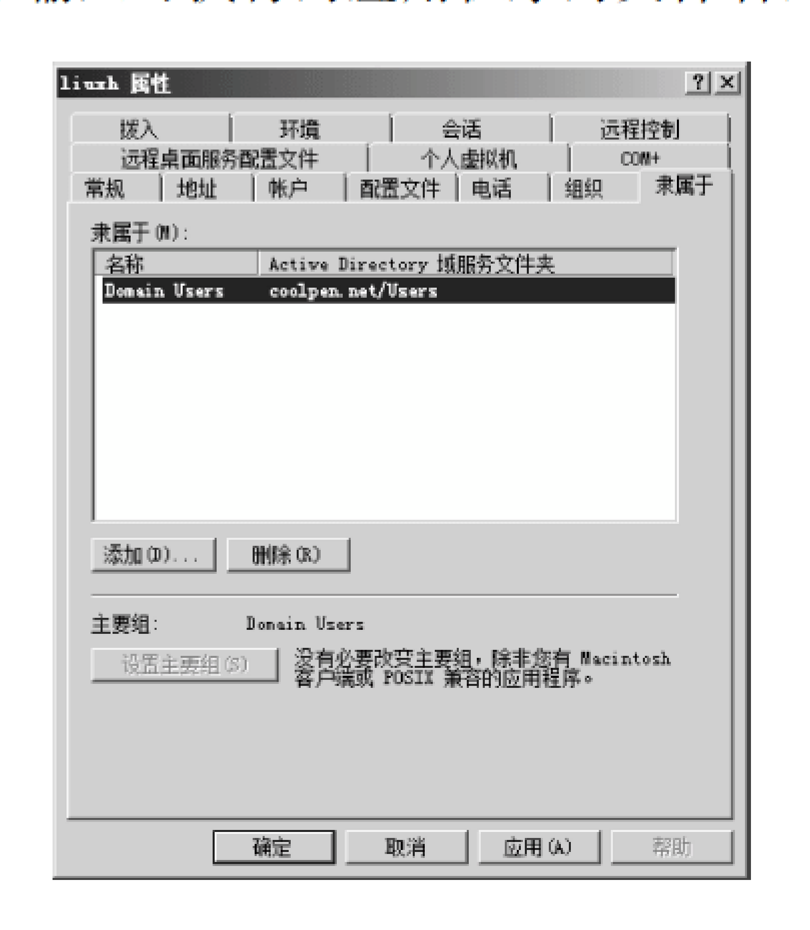


图 9-106　“隶属于”选项卡

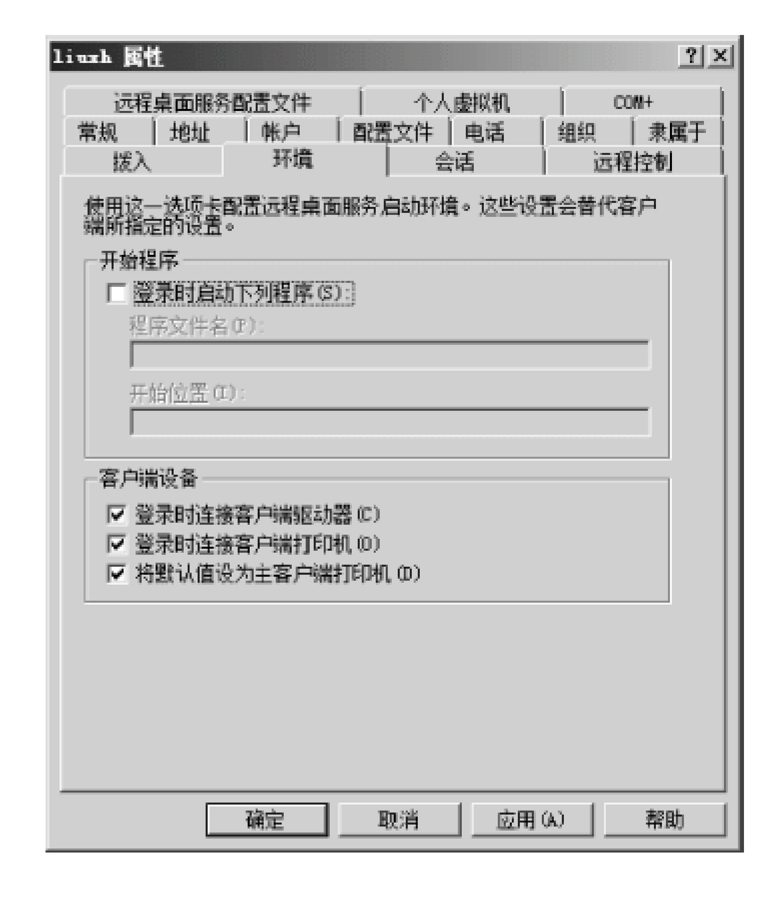


图 9-107　“环境”选项卡

在“客户端设备”选项区域中包含如下复选框。

① “登录时连接客户端驱动器”复选框：仅作用于启用了终端服务器会话中使用重新映射的客户驱动器的会话，映射的驱动器在“Windows 资源管理器”中显示为“其他驱动器”。

② “登录时连接客户端打印机”复选框：用于指定任何从终端服务器会话映射的打印机都应该被重新连接。

③ “将默认值设为主客户端打印机”复选框：用于指定客户端应该使用的是本地的默认打印机，而不是终端服务器定义的打印机。

3. 禁用、启用、重命名和删除用户账户

以具有管理员权限的账户登录控制器，打开“Active Directory 用户和计算机”窗口，右

击想要禁用的用户账户，选择快捷菜单中的“禁用账户”命令即可将其禁用，如图 9-108 所示。

用户账户被禁用以后，便不能再登录。如果想启用用户账户，则可以按照相同的方法，选择快捷菜单中的“启用账户”命令即可。如果账户不再使用，或需要重设所有权限，可将其删除，右击用户账户名，并选择快捷菜单中的“删除”命令即可删除该账户。

4. 重置口令与解除锁定用户账户

在域环境中重设账户密码比较简单。使用具有相关权限的管理员账户登录到域控制器，打开“Active Directory 用户和计算机”窗口。选择 Users 选项，右击想要重置密码的用户账户，选择快捷菜单中的“重置密码”命令，显示图 9-109 所示的“重置密码”对话框，在“新密码”和“确认密码”文本框中输入新密码，单击“确定”按钮即可。使用这种方法，也可以重设管理员账户的密码。



图 9-108 禁用域用户账户



图 9-109 “重置密码”对话框

如果当前账户已被锁定，则可以选中“解锁用户的账户”复选框，使密码更改立即生效。系统默认配置的安全策略，可能会限制用户更改密码的次数或登录次数，如果超出策略限制，则立即锁定账户，并等待一定时间后自动解锁。此时，对应用户可以告知管理员，由管理员登录到域控制器，为其重设密码并解锁账户。

9.5.2 组的管理

域中的组可以包含用户、计算机、联系人、组等目录对象，基本管理任务包括创建与删除组、设置组管理员、更改组类型和作用域、设置组访问权限等。

1. 创建组

在域中，只有拥有管理员权限，或者被委派了相关权限的用户账户，才可以登录到域控制器创建组。

打开“Active Directory 用户和计算机”窗口，选择新建组所在的 OU 或容器，在窗口空白处右击，选择快捷菜单中的“新建”→“组”命令，显示图 9-110 所示的“新建对象 - 组”对话框。在“组名”文本框中，输入需要新建组的名称，如：student；在“组名(Windows 2000 以前版本)”文本框中，系统自动完成对应的组名；在“组作用域”选项区域中选中“全局”单选按钮；在“组类型”选项区域中选中“安全组”单选按钮。单击“确定”按钮，完成安全用户组

的创建。

2．为组指定管理员

组管理员只是针对域用户组而言的，独立服务器不具有此功能。在独立服务器系统中，只有管理员账户可以管理所有用户组，如更新成员列表、更改账户权限等。而在域中，可以为组指定特定的管理者，使其可以完成组中成员的某些工作，如权限委派等。需要注意的是，默认情况下，指定组管理员后，其他任何用户甚至管理员都将无法管理该组。

（1）打开“Active Directory 用户和计算机”控制台，选择要指定管理员的组，如 coolpen，右击并选择快捷菜单中的“属性”命令，显示“coolpen 属性”对话框，选择图 9-111 所示的“管理者”选项卡。



图 9-110 “新建对象 - 组”对话框

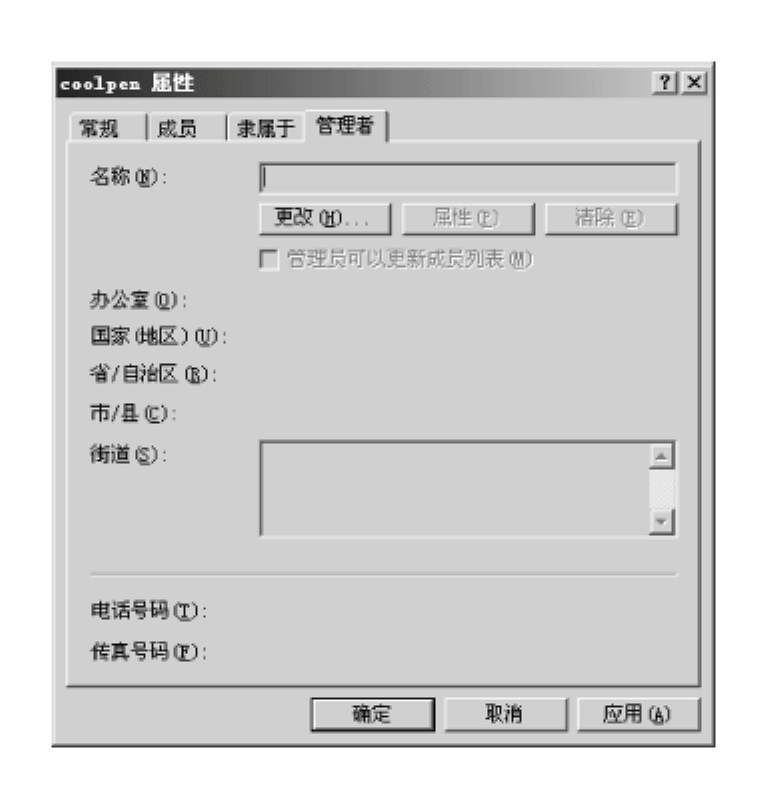


图 9-111 “管理者”选项卡

（2）单击“更改”按钮，显示图 9-112 所示的“选择用户、联系人或组”对话框。在“输入要选择的对象名称(例如)”文本框中，输入要指派的管理者的用户名或组名。需要注意的是，这里只能选择一个管理者。

（3）单击“确定”按钮，返回“管理者”选项卡，在“名称”文本框中，显示了所添加的管理者用户名称，如图 9-113 所示。如果要清除管理者用户账户，单击“清除”按钮即可。



图 9-112 “选择用户、联系人或组”对话框

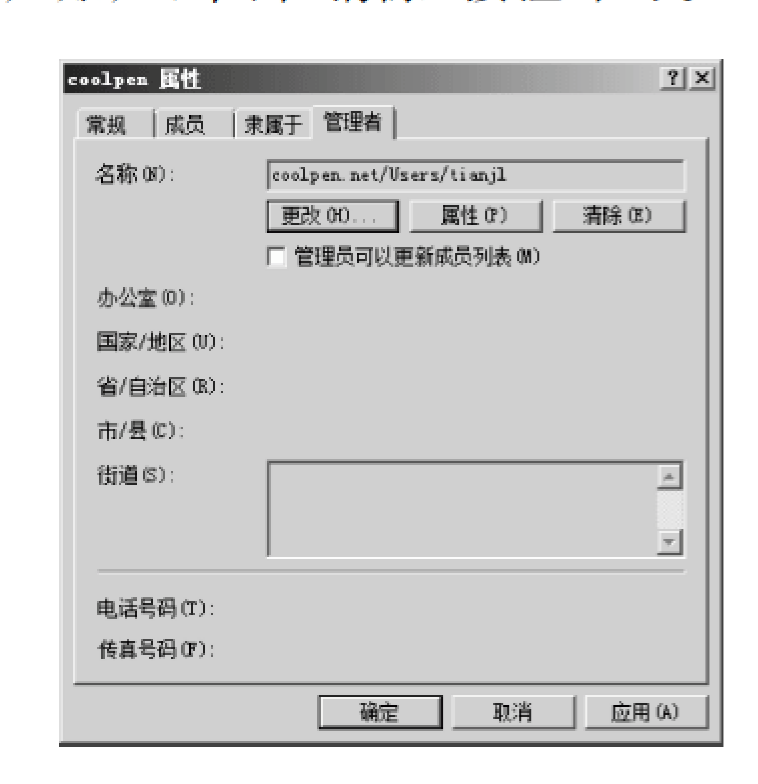


图 9-113 已指定管理者

小知识：默认情况下，“管理员可以更新成员列表”复选框没有被选中，表示只有被指定的管理者才能管理该组，即使是域管理员也无此权限。如果选中该复选框，则允许管理员账户更新组成员列表。

(4) 单击"确定"按钮,完成组的管理者的指派。

3. 更改组作用域或组类型

组作用域直接决定组中账户的应用范围,而组类型则决定用户账户可以行使的功能。应用过程中,管理员可以根据需要更改域用户组的作用域和类型。Windows Server 2008 R2 系统的默认域功能级别为 Windows Server 2003,并且已经删除了 Windows 2000 混合模式,所以可以直接更改。

打开"Active Directory 用户和计算机"控制台,双击欲更改的用户组(以 coolpen 组为例),显示图 9-114 所示的"coolpen 属性"对话框,在"常规"选项卡的"组作用域"和"组类型"选项区域,重新选中指定的单选按钮即可。

4. 删除组

在"Active Directory 用户和计算机"窗口中,右击要删除的组并选择快捷菜单中的"删除"命令,即可删除该组。需要注意的是,随着用户组的删除,通过该组所赋予成员账户的权限也会被删除,但组内的成员不会被删除。

5. 授予组访问权限

在"A-G-DL-P"规划原则中,授权是最后一步。所谓"授权"是指根据用户身份授予用户账户访问网络资源的权限,例如读取、更改、完全控制等。以 software 共享文件夹为例,设置 coolpen 组的访问权限。

(1) 右击 software 文件夹,在快捷菜单中选择"属性"命令,显示"software 属性"对话框,选择"共享"选项卡。

(2) 单击"高级共享"按钮,显示图 9-115 所示的"高级共享"对话框。在"共享名"文本框中,可以设置当前共享文件夹的共享名。



图 9-114 "coolpen 属性"对话框



图 9-115 "高级共享"对话框

(3) 单击"权限"按钮,显示"software 的权限"对话框。目前,Everyone 组拥有该共享文件夹的读取权限。

(4) 单击"添加"按钮,显示图 9-116 所示的"选择用户、计算机、服务账户或组"对话框,在"输入对象名称来选择(示例)"文本框中,输入 coolpen,单击"检查名称"按钮验证输入是否正确。

（5）单击“确定”按钮，将 coolpen 组添加到“组或用户名”列表中，如图 9-117 所示。选中该组，可以在“coolpen 的权限”列表中设置其访问权限。

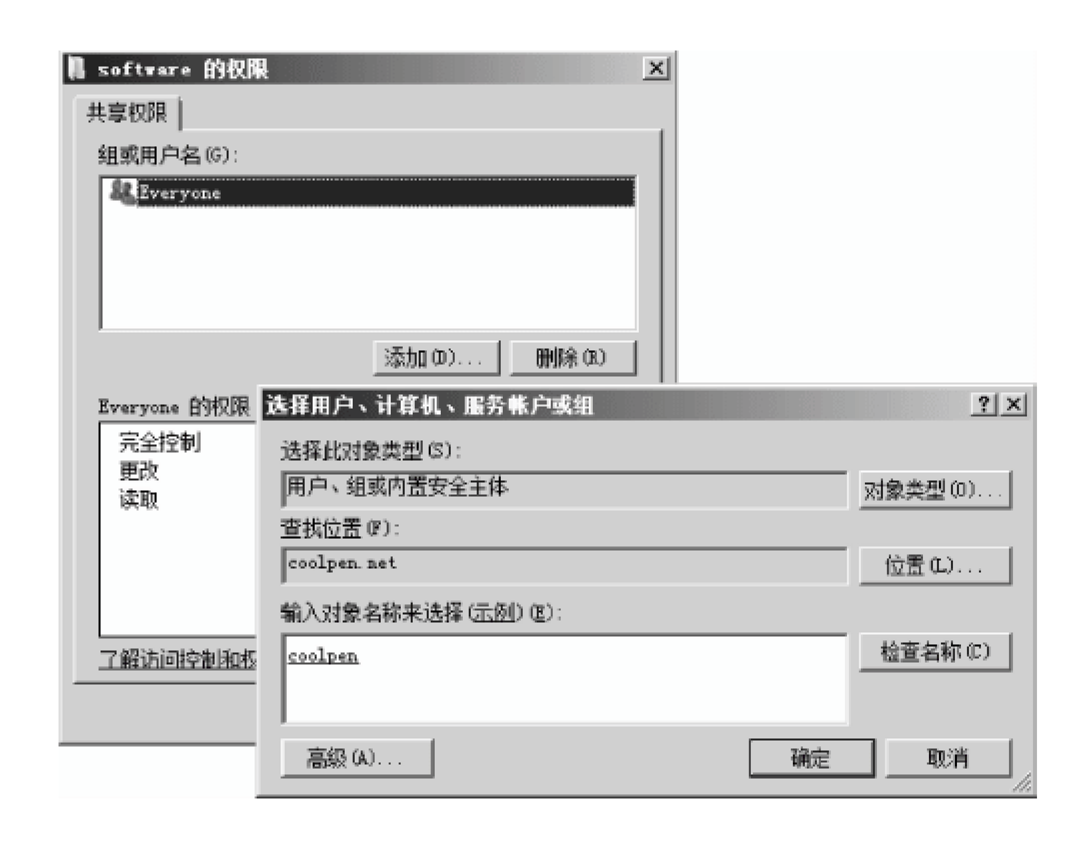


图 9-116　“选择用户、计算机、服务账户或组”对话框



图 9-117　授予 coolpen 组访问权限

（6）连续单击“确定”按钮，完成 coolpen 组访问权限的授权。

9.5.3　知识链接：用户账户与组概述

1. 用户账户概述

用户账户可以分为两种类型：本地用户账户和域用户账户。“本地用户账户”只能用于登录和管理本地计算机；“域用户账户”可以登录到域并使用域管理员允许其访问的所有网络资源。下面主要介绍域用户账户的管理。

（1）用户账户类型

在 Active Directory 中，域用户账户可以分为以下几种身份：标准域用户账户、域管理员账户、企业管理员账户。

① 标准域用户账户。标准域用户账户是域中应用最多的用户账户，对应于网络中的所有用户。默认创建的域用户账户将被添加到“Users”组中。在不同的 OU 中创建的标准域用户账户性质相同，使用同一个默认的密码策略。标准域用户账户可以被添加到不同的组中，但是只能在一个 OU 中。

② 域管理员账户。域管理员账户是具备管理权限的特殊用户账户。AD DS 域服务部署完成后，默认的域管理员账户为 Administrator。域管理员账户拥有网络中较高的权限，拥有管理员权限，也就相当于基本拥有了整个网络的完全控制权。

③ 企业管理员账户。在 Active Directory 中，具备最高管理权限的用户账户不是 Administrators 和 Domain Admins 组中的成员，而是 Enterprise Admins 组中的成员。默认的管理员账户 Administrator 是 Enterprise Admins 组中的成员，也是唯一的成员。因此，默认的管理员账户 Administrator 具备企业的最高管理权限。正是由于 Windows 系统的这一默认设置，使得 Administrator 成为黑客攻击的首要对象。建议将 Administrator 管理员账户降级为普通的用户，使其具备最低的权限，禁止或者重命名此账户。创建一个新的账户，使其具备 Active Directory 中最高的管理权限。

（2）用户账户的功能

当网络中的用户需要通过自己的计算机登录到域时，其必须有一张被域控制器认可的“身份证”，这张身份证在域中就是用户账户。在域中创建和管理用户的操作必须在域控制器中进行。用户账户主要有如下功能。

① 验证用户或计算机的身份：用户能够利用经域验证后的标识登录到计算机和域。登录到网络的每个用户应有自己的唯一账户和密码。为了获得最高的安全性，应避免多个用户共享同一个账户。

② 授权或拒绝访问域资源：一旦用户已经通过身份验证，那么就可以根据指派给该用户的关于资源的显式权限，授予或拒绝该用户访问域资源。

③ 管理其他用户：在本地域中可以使用委派控制，允许对某个用户进行单独的权限委派，例如，使某个用户具备更改其他用户密码的权限。

④ 审核使用用户或计算机账户执行的操作：审核有助于监视账户的安全性。

（3）命名惯例

在企业网络中，除了每个人有一个用户外，还可能有为此用户对应提供的一些服务，如企业电子邮件服务、企业办公自动化的登录账户等。为了便于管理，建议使用统一的方式进行命名，一是让计算机的使用者记住自己的用户名；另外，通常用户名还与企业为其提供的电子邮件相对应。域用户账户命名管理规则如下。

① 对于每个使用者，通常都是使用其“姓”的全称加上“名”的简称作为账户名，例如，刘晓辉的用户账户名为 liuxh。

② 如果使用简称之后有“重名”的现象，可以对重名的用户使用全称或者加序号标识，例如 liuxh01。

（4）密码要求

密码是用户登录网络的钥匙，密码是否安全直接影响到用户的信息是否安全。账户密码应当定期修改，尤其是当发现有不良攻击时，更应及时修改为复杂密码，以免被破解。为避免密码因过于复杂而忘记，可用笔记录下来，并保存在安全的地方，或随身携带避免丢失。

综上所述，若欲保证密码的安全，应当遵循以下规则。

① 用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符。建议将这些符号排列组合使用，以期达到最好的保密效果。

② 用户密码不要太规则，不要使用用户姓名、生日、电话号码以及常用单词作为密码。

③ 根据 Windows 系统密码的散列算法原理，密码长度设置应超过 7 位，最好位数为 14 位或者更长。

④ 密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘中，且包含密码的文件是只读的。

⑤ 密码应定期修改，且避免重复使用旧密码，应采用多套密码的命名规则。

⑥ 启用账户锁定机制。一旦同一账户密码校验错误若干次即断开连接并锁定该账户，经过一段时间才解锁。

Windows Server 2008 和 Windows Server 2008 R2 对更改密码的要求非常严格。默认情况下密码策略要求如下。

① 密码必须符合复杂性要求。

② 密码长度至少为7个字符。

③ 密码最短使用时间为1天。

④ 密码最长使用期限为42天。

⑤ 不得使用历史密码,默认记录24个历史密码。

2. 组概述

域中的组有多种类型,并且可以根据需要设置组的作用域。不同类型和作用域的组,其成员属性设置也会有所不同。

(1) 组类型

在Active Directory中有两种类型的组:通信组和安全组。使用通信组可以创建电子邮件通信组列表;使用安全组则可给共享资源指派权限。组有以下特点。

- 对组设置的权限将自动应用到组中的所有对象上,可以大大简化管理员的工作。
- 组可以位于Active Directory中,也可以位于本地的独立计算机中。
- 组属性由作用域和类型决定。
- 可以嵌套,即可以将一个组添加到另一个组中。

① 通信组。在电子邮件应用程序中,管理员可以使用"通信组"将电子邮件同时发送给一组用户。通信组不使用Windows Server的安全机制,但是可以在"对象访问控制列表"中出现。如果需要使用组来控制对共享资源的访问,则需要使用安全组。

② 安全组。安全组提供了一种有效的方式来指派对网络上资源的访问权。与通信组不同,安全组可以使用Windows Server的安全机制,并且可以根据需要添加到随机访问控制列表中。使用安全组,可以带来以下的功能方面的安全性。

- 将用户权利指派到Active Directory中的安全组。管理员可以对安全组指派用户权利,以确定该组的哪些成员可在域(或林)作用域内工作。在安装Active Directory时,系统会自动将用户权利指派给某些安全组,以帮助管理员定义域中人员的管理角色,例如,在Active Directory中,被添加到Backup Operators组的用户,能够备份和还原域中每个域控制器上的文件和文件夹。因为在默认情况下,系统已经将备份和还原目录的用户权利自动指派给Backup Operators组,组中的用户继承该组的用户权利设置。可以使用组策略将用户权利指派给安全组,以帮助委派特定任务。在指派委派的任务时应始终谨慎操作,避免为非必要用户指派过高的权利,以免产生安全隐患。
- 给安全组指派对资源的权限。用户权利和权限不应混淆。对共享资源的权限将指派给安全组。权限决定了哪些用户可以访问该资源以及访问的级别,例如,是读取还是完全控制。系统将自动指派域对象的某些权限,以允许对默认安全组(例如Account Operators组或Domain Admins组)进行多级别的访问。在定义对资源和对象的权限的ACL中列出了安全组。为资源指派权限时,管理员应将权限指派给安全组而非单个用户。权限可以直接指派到组,而不是逐个指派给组中单独的用户。添加到组的每个账户,都将接受在Active Directory中指派给该组的权利,以及在资源上为该组定义的权限。

③ 安全组和通信组之间的转换。域功能级别设置为Windows Server 2003、Windows Server 2008或Windows Server 2008 R2模式时,管理员可以将安全组转换为通信组,反之亦然。在Windows Server 2003系统中,域功能级别还包括Windows 2000混合模式,设置

为域功能级别时,安全组和通信组之间不能转换。

(2) 组作用域

组的作用域决定了组的作用范围、组中可以拥有的成员以及组之间的嵌套关系。在Windows Server 2008域模式下组有3种组作用域:全局、本地域和通用。

- 通用组的成员:可以包括域树或林中任何域中的其他组和账户,而且可在该域树或林中的任何域中指派权限。
- 全局组的成员:可以包括只在其中定义该组的域中的其他组和账户,而且可在林中的任何域中指派权限。
- 本地域组的成员:可以包括Windows Server 2008 R2、Windows Server 2008、Windows Server 2003、Windows 2000域中的其他组和账户,且只能在域内指派权限。

① 本地域组。具有本地域作用域的组将帮助定义和管理对单个域内资源的访问。这些组可将以下组或账户作为其成员。

- 具有全局作用域的组。
- 具有通用作用域的组。
- 账户。
- 具有本地域作用域的其他组。
- 上面任意组的组合。

② 全局组。所谓"全局"就是指整个域,此类组属于某个指定域,但作用域确是整个森林。全局组的成员只能是在本地的域中,可以访问在森林任何域里的资源。全局组只能放置在同一个域中的资源对象安全描述符中,即不能只是基于另一个域的全局组用户成员身份,而限制对相应对象的访问。在用户登录到一个域时,用户的全局组成员身份将被评估。因为全局组成员身份是以域为中心的,所以全局组成员身份的更改不会强行复制到整个企业范围的全局编录中。在"本机模式"域中,全局组可相互嵌套。

管理员只能在创建该全局组的域上进行添加用户账户和全局组,而且全局组可以嵌套在其他组中。可以将某个全局组添加到同一个域上的另一个全局组中,或添加到其他信任域的通用组和本地域组中(不能加入到不同域的全局组中,全局组只能在创建它的域中添加用户和组)。虽然可以利用全局组授予访问任何域上的资源的权限,但一般不直接用它进行权限管理。

③ 通用组。使用具有通用作用域的组可以合并跨越不同域的组,所以,可以将账户添加到具有全局作用域的组,并且将这些组嵌套在具有通用作用域的组内。使用该策略,对具有全局作用域的组中的任何成员身份的更改都不影响具有通用作用域的组。

具有通用作用域的组成员身份不应频繁更改,因为对这些组成员身份的任何更改都将引起整个组的成员身份复制到树林中的每个全局编录中。

④ 更改组作用域。在默认情况下,新建组将被配置为具有全局作用域的安全组,而与当前域功能级别无关。在Windows Server 2008 R2系统的域中,允许对组作用域进行如下转换。

- 全局到通用。只有当要更改的组不是另一个全局作用域组的成员时,才允许进行该转换。
- 本地域到通用。只有当要更改的组没有另一个本地域组作为其成员时,才允许进行

该转换。

- 通用到全局。只有当要更改的组没有另一个通用组作为其成员时，才允许进行该转换。
- 通用到本地域。该操作没有限制。

(3) 组设计原则

域中的组有多种类型，并且根据作用域的不同，其功能也会有所不同。因此，应用组管理目录对象之前，必须经过严格的规划和设计。组的基本属性就是所包含对象具有的基本属性，例如同属某一部门或同在某一地区的用户、某一部门的计算机、网络中的打印机等具有相同的属性。除此之外，设计组的过程中还应遵循“A-G-DL-P”原则。

① A：建立一个“全局组”，然后将具备相同权限的用户账户加入到此组内，例如，将教务处内所有教务员账户加入到一个称为 TEACH 的“全局组”内。

② G：建立一个“本地域组”，可以设置让此组对某些资源具备适当的权限，例如教务处的激光打印机只能提供某些用户来使用，则可以建立一个 PRINTER 的“本地域组”。

③ DL：将所有即将拥有权限访问此资源的“全局组”加入到“本地域组”内，例如将 TEACH“全局组”加入到此本域组内。

④ P：指定适当的权限给此“本地域组”，例如，给予 PRINTER“本地域组”对此激光打印机具备打印的权限。

以上 4 个步骤称为“A-G-DL-P”原则。简言之，就是将用户账户加入到“全局组”内，将此“全局组”加入到“本地域组”内，指派适当的权限给此“本地域组”。

提示：A：Account，用户账户；G：Global Group，全局组；DL：Domain Local Group，域本地组；P：Permissions，授权。

例如，某公司的网络中有两个域：coolpen. net 和 hsnc. cn。

coolpen. net 域中的 5 个用户和 hsnc. cn 域中的 3 个用户都需要访问 hsnc. cn 域中的 software 文件夹。

下面以两种方式进行组的规划。

① 无原则规划。可以在 hsnc. cn 域中建一个“本地域组”，因为“本地域组”的成员可以来自所有的域，然后把这 8 个用户都加入这个“本地域组”，并把 software 文件夹的访问权赋给“本地域组”。

这种规划方式的缺点：因为 DL 是在 hsnc. cn 域中，所以，管理权也在 hsnc. cn 域。如果 coolpen. net 域中的 5 个用户变成 6 个用户，只能是 coolpen. net 域管理员通知 hsnc. cn 域管理员，将“本地域组”的成员做一下修改，hsnc. cn 域的管理员没有管理的权利。

② 按照 A-G-DL-P 原则规划。在 coolpen. net 域和 hsnc. cn 域中都各建立一个“全局组”(G)，然后在 hsnc. cn 域中建立一个“本地域组”，把这两个“全局组”都加入 hsnc. cn 域中的“本地域组”中，然后把 software 文件夹的访问权赋给“本地域组”。两个“全局组”都有权访问 software 文件夹。

这种规划方式的优点：组嵌套造成权限继承。两个“全局组”分布在 coolpen. net 域和 hsnc. cn 域中，也就是 coolpen. net 域和 hsnc. cn 域的管理员都可以自己管理自己的“全局组”，只要把那 5 个用户和 3 个用户分别加入“全局组”中，就可以管理对 software 文件夹的访问。如果需要添加用户或者做其他任何修改，由域的管理员独立完成。

习题

1. 简述 Sniffer 的功能。
2. 简述 IPMaster 的功能。
3. 简述域用户账户类型。
4. 域用户账户有哪些功能?
5. Windows Server 2008 的默认密码策略有哪些?

实验:创建并访问共享文件夹

实验目的:

掌握共享文件夹的创建与访问方法。

实验内容:

通过不同方法设置共享文件夹,使用不同方法访问共享文件夹。

实验步骤:

(1) 在文件服务器中设置共享文件夹 share1。

(2) 在资源管理器中设置共享文件夹 share2。

(3) 在控制台树中设置共享文件夹 share3。

(4) 使用不同方法访问共享文件夹。

第 10 章 chapter 10

网络安全管理

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。但由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互联性等特征，致使网络容易受到来自黑客、恶意软件和其他种种攻击，从而使网上信息安全成为一个令人头痛的问题，因此，排除自然和人为等诸多因素造成的网络脆弱性和潜在威胁，确保网络信息的保密性、完整性和可用性，成为网络管理员要做的头等大事。

10.1 网络安全规划

没有安全意识的管理员是无法保证网络安全的，因此，作为管理员需要对网络的不同部分分别进行安全设计，包括网络设备安全规划、网络安全设备规划、客户端安全规划。

10.1.1 网络设备安全规划

交换机和路由器是几乎所有局域网络都要使用的基本设备。交换机将其他网络设备(如集线器、交换机和路由器等)和所有终端设备(如计算机、服务器和网络打印机等)连接在一起，实现彼此之间的通信；路由器用于实现局域网之间，以及局域网与 Internet 之间的互联。

1. 交换机安全规划

交换机是搭建局域网络时不可或缺的集线设备，其主要功能就是连接设备和隔离网络中的碰撞。

(1) 风暴控制

当端口接收到大量的广播、多播或单播包时，就会发生广播风暴。转发这些包将导致网络速度变慢或超时。借助对端口的广播风暴控制，可以有效地避免因硬件损坏或链路故障而导致的网络瘫痪。默认状态下，广播、多播或单播包风暴控制被禁用。

(2) 流控制

流控制只适用于 1000Base-T、1000Base-SX 和 GBIC 端口。在千兆端口启用流控制后，可以在拥塞期间暂停其他终端的连接。当端口处于拥塞状态无法接收到数据流时，将通知其他端口暂停发送，直到恢复正常状态。当本地设备发现任何终端发生拥塞时，将发送一个暂停帧，以通知其连接伙伴或远端拥塞设备。当收到暂停帧后，远程设备将停止发送任何数据包，以防止在拥塞期内丢失任何数据包。

注意：当交换机配置有 QoS(Quality of Service)时，不要再配置 IEEE 802.3X 流控制。

(3) 保护端口

保护端口(Protected Port)可以确保同一交换机上的指定端口之间不进行通信。保护端口不向其他保护端口转发任何传输,包括单播、多播和广播包。传输不能在第二层保护端口间进行,所有保护端口间的传输都必须通过第三层设备转发。保护端口与非保护端口间的传输不受任何影响。

(4) 安全端口

借助安全端口可以只允许指定的 MAC 地址或指定数量的 MAC 地址访问某个端口,从而避免未经授权的计算机接入网络,或限制某个端口所连接的计算机数量,从而确保网络接入的安全。

(5) 绑定 IP 和 MAC 地址

许多安全设置都是基于 IP 的,而用户的 IP 地址却可以自动或手动随意设置。因此,还应当同时采取另外一种安全措施,即在交换机中将 IP 地址与 MAC 地址绑定在一起。这样,即使用户设置了 IP 地址,也由于 MAC 地址不同而不能获得相应的权限,从而保证网络的安全。

2. 路由器安全规划

路由器是一种智能选择数据传输路由的设备,用于连接多个相同或不同类型的局域网络。以路由器为基础构建(Router Based Network)的网络被称为“网间网”,例如企业与其分支机构之间构建的网络,甚至城域网络等都属于“网间网”的范畴。事实上,几乎每天都要使用的 Internet 就是由数以万计的路由器构建而成的、超大规模的、具有国际性的“网间网”。

(1) 访问控制列表

访问控制列表(Access Control List,ACL)是 Cisco IOS 提供的一种访问控制技术,被广泛应用于路由器和三层交换机。借助 ACL,可以有效地控制用户对网络和 Internet 的访问,从而最大限度地保障网络安全。

Cisco 支持 3 种类型的访问列表,即标准 IP 访问控制列表、扩展 IP 访问控制列表和命名访问控制列表。

① 标准 IP 访问控制列表。标准 IP 访问控制列表只允许过滤源地址,且功能十分有限。当想阻止来自某一网络的所有通信流量,或者允许来自某一特定网络的所有通信流量,或者想要拒绝某一协议簇的所有通信流量时,可以使用标准 IP 访问控制列表来实现这一目标。标准 IP 访问控制列表检查路由的数据包的源地址,从而允许或拒绝基于网络、子网或主机的 IP 地址的所有通信流量通过路由器的出口。

② 扩展 IP 访问控制列表。扩展 IP 访问控制列表允许过滤源地址、目的地址和上层应用数据,因此,可以适应各种复杂的网络应用。扩展 IP 访问控制列表既检查数据包的源地址,也检查数据包的目的地址,还检查数据包的特定协议类型、端口号等。扩展 IP 访问控制列表更具有灵活性和可扩充性,即可以对同一地址允许使用某些协议的通信流量通过,而拒绝使用其他协议的流量通过。

③ 命名访问控制列表。在标准与扩展 IP 访问控制列表中均要使用表号,而在命名访问控制列表中使用一个字母或数字组合的字符串来代替前面所使用的数字。使用命名访问控制列表可以删除某一条特定的控制条目,这样,可以在使用过程中方便地进行修改。

在设置访问列表时,应当遵循最小特权原则,即只给受控对象完成任务所必需的最小权

限，从而最大限度地保障网络传输安全。所谓最小特权(Least Privilege)是指在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权。最小特权原则是指应限定网络中每个主体所必需的最小特权，确保可能的事故、错误和网络部件的篡改等原因造成的损失最小。最小特权原则一方面给予主体必不可少的特权，保证所有的主体都能在所赋予的权限内完成自己的任务或操作；另一方面，只给予主体必不可少的特权，从而限制每个主体所能进行的操作，以确保企业网络安全。

① 自上而下的处理过程。访问列表包含一个访问控制条目(Access Control Entry, ACE)规则列表。每个 ACE 都指定 Permit(允许)或 Deny(拒绝)，以及应用条件，报文会逐个条目顺序匹配 ACE。访问列表表项的检测按自上而下的顺序进行，并且从第一个表项开始。这意味着必须特别谨慎地考虑访问列表中语句的顺序。

当一个报文在一个接口上被接收到时，交换机将报文中的相关字段与应用于该接口上的 ACL 进行比较，验证该报文是否满足该 ACL 的所有 ACE 的转发条件。交换机对该 ACL 的所有 ACE 进行逐条比较，当第一个匹配的条件找到时(该报文与某一条 ACE 的匹配条件完全匹配)决定对该报文是接收(Accepts)还是拒绝(Rejects)。因为交换机在找到第一个匹配条件时就停止比较，因此接入控制列表的匹配条件的顺序是至关重要的，在进行 ACL 的配置时应给予关注，否则配置可能不一定如愿。如果所有条件都不匹配，则交换机拒绝该报文。如果没有任何对此报文的限制条件，则交换机转发该报文，否则丢弃之。关于该规则，以 A 国的《海关过境规则》来理解。当一个入关人员从某一个海关入境时，海关工作人员将其与《海关过境规则》中的所有细则从头到尾相比较，当某一条细则与入关人员身份匹配时，则该入关人员就适用于该细则的待遇。由于是按照过境规则从头到尾比较，因此细则的顺序是至关重要的，比如，细则第一条为：携带危险物品者拒绝入境，如果将该细则放到最后，则可能有些携带危险物品者也符合别的细则的身份要求而被当作允许入境人员而入境。所以该细则一定要放在过境规则的第一条。另外，海关过境规则的所有细则申明了所有允许入境人员的适用条件，不符合所有细则的入境人员均被视为非法入境人员。同理，交换机接口上接收到的报文，如果不匹配该接口上 ACL 的所有 ACE 的匹配条件，则该报文被视为非法报文而被丢弃。可以通过在 ACL 的最后添加一条允许所有报文的 ACE 以允许其他所有报文通过。

ACL 的 ACE 是按照生成 ACE 的顺序从第一条开始往后添加的，不能有选择地将某一条 ACE 添加到某一个 ACL 的某一个指定位置。但可以通过 no 命令来删除某一条 ACE。如果一条 ACL 已经被关联到某一个接口上，则对该 ACL 所做的修改会被重新应用到该接口上。但由于硬件资源表项的限制，重新应用可能导致资源不足而失败。

如果将一条没有任何 ACE 的 ACL 应用到某一个接口上，则意味着允许所有报文通过，即 Permit any。

② 添加表项。新增加的表项被追加到访问列表末尾，这就意味着不能改变已有的访问列表的功能。如果要改变，就必须创建一个新的访问列表，删除已经存在的访问列表，并且将新的访问列表应用于接口上。

③ 标准访问列表过滤。标准访问列表只限于过滤源地址，所以，需要使用扩展的 IP 访问列表来满足企业的特殊需求。

④ 访问列表位置。应当将扩展访问列表尽量放在靠近过滤源的位置上，这样，创建的

过滤器就不会反过来影响其他接口上的数据流。而标准访问列表则应当尽量靠近目的地的位置。由于标准访问列表只使用源地址,因此,将阻止报文流向其他端口。

⑤ 语句的位置。由于 IP 协议包含 ICMP、TCP 和 UDP,所以,应当将具体的表项放在不太具体的表项前面,以保证位于另一个语句前面的语句不会否定表中后面语句的作用效果。

⑥ 访问列表应用。使用 Access-group 命令应用访问列表。需要注意的是,只有访问列表被应用于接口上时,才执行过滤操作,从而真正产生作用。

⑦ 过滤方向。通过接口的数据流是双向的。过滤方向定义了要检查的是流入还是流出的报文。所以,访问列表要应用到接口的特定方向上。向外的(Outbound)表示数据流从三层设备流出;向内的(Inbound)表示数据流流向三层设备。

⑧ ACL 与系统中其他的应用互斥。如果打开某一个端口的 802.1x 认证功能,而又将某一个 ACL 关联到某一个接口,虽然系统并不报错,但该 ACL 将不会生效。如果配置某一个端口的安全地址时选择了 IP 地址选项,而又将某一个 ACL 关联到某一个接口,虽然系统并不报错,但该 ACL 将不会生效。

访问列表配置步骤如下。

① 分析需求,搞清楚需求中要保护什么或控制什么;为方便配置,最好能以表格形式列出。

② 分析符合条件的数据流的路径,寻找一个最适合进行控制的位置。

③ 编写 ACL,并将 ACL 应用到接口上。

④ 测试并修改 ACL。

(2) NAT

借助于 NAT,私有(保留)地址的"内部"网络通过路由器发送数据包时,私有地址被转换成合法的 IP 地址,从而只需使用少量 IP 地址(甚至是 1 个),即可实现私有地址网络内所有计算机与 Internet 的通信。也就是说,在网络内的计算机数量大于 ISP 提供的合法 IP 地址时,NAT 就拥有了自己的用武之地。

NAT 将自动修改 IP 报文头中的源 IP 地址和目的 IP 地址,IP 校验则在 NAT 处理过程中自动完成。有些应用程序将源 IP 地址嵌入到 IP 报文的数据部分中,所以,还需要同时对报文进行修改,以匹配 IP 头中已经修改过的源 IP 地址。否则,在报文数据部分嵌入 IP 地址的应用程序就不能正常工作。令人遗憾的是,尽管 NAT 的 Cisco 版本可以处理许多应用,但它毕竟不是万能的,还是有些应用无法被支持。表 10-1 列举了 Cisco NAT 支持的和不支持的应用。

NAT 的实现方式有 3 种,即静态转换、动态转换和端口多路复用。

① 静态转换:指将内部网络的私有 IP 地址转换为公用 IP 地址时,IP 地址对是一对一的,是一成不变的,某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换,可实现外部网络对内部网络中某些特定设备(如服务器)的访问。

② 动态转换:指将内部网络的私有 IP 地址转换为公用 IP 地址时,IP 地址对是不确定的,是随机的,所有被授权访问 Internet 的私有 IP 地址,可随机转换为任何指定的合法 IP 地址。也就是说,只要指定哪些内部地址可以进行转换,以及用哪些合法地址作为外部地址时,就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时,可以采用动态转换的方式。

表 10-1 Cisco NAT 支持的和不支持的应用

支持的应用	不支持的应用
任何非源和目的的 TCP/UDP 报文	IP 组播
在 IP 报文的数据部分中的 IP 地址	路由表更新
ICMP	DNS 域的迁移
FTP	BOOTP
TCP 上的 NetBIOS(会话服务除外)	Talk,NTalk
RealAudio	SNMP
White Pines CUSeeMe	NetShow
Streamworks	
DNS(A 查询和 PTR 查询)	
H. 323	
NetMeeting	
VDOLive	
Vxtreme	

③ 端口多路复用:指改变外出数据包的源端口并进行端口转换完成,即端口地址转换(Port Address Translation,PAT)。采用端口多路复用方式,内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问,从而可以最大限度地节约 IP 地址资源。同时,又可隐藏网络内部的所有主机,有效避免来自 Internet 的攻击。因此,目前网络中应用最多的就是端口多路复用方式了。

10.1.2 网络安全设备规划

网络安全设备有多种类型,防火墙就是其中一种,防火墙通常部署于网络的边界。当然,边界可以是局域网与广域网的、局域网与 Internet 的、不同子网之间的,以及子网与服务器之间的等。

对于安全设备的配置与管理,通常在对安全设备进行初始化后,使用 Cisco ASDM 进行日常管理和配置比较方便。对于 Cisco ASDM 的安装,需要在安全设备和管理计算机上同时安装。另外,建议将 Cisco ASDM 的安装程序保存到安全设备上,在客户端计算机登录设备时,即可使用该安装程序将 Cisco ASDM 安装到计算机上。

10.1.3 客户端安全规划

虽然在客户端计算机上通常不会保存有高保密性的文件,但往往由于客户端计算机的安全性不高,而使其成为攻击者用来攻击服务器的跳板。因此,客户端计算机的安全同样需要管理员足够的重视。

对于客户端计算机的安全,通常采用的方法是启用防火墙和系统自动更新,并在离开计算机时锁定计算机,防止其他人窥视隐私文件。

10.2 网络设备安全管理

交换机和路由器是计算机网络最常用的网络设备,其安全性将直接影响到整个网络的可用性和稳定性,对于网络安全起着至关重要的作用。尤其是网络路由器,作为局域网中唯

一暴露在 Internet 中的设备,更是常常经受恶意攻击。路由器和交换机一旦被攻破,网络安全和正常运行也就无从谈起了。

10.2.1 交换机安全管理

作为网络传输枢纽的交换机,在网络安全中的重要地位是无可取代的。无论是控制广播风暴的产生、拒绝用户之间非授权访问、限制用户的网络服务与应用、禁止未授权计算机接入网络还是拒绝非法用户访问网络,都离不开对交换机的安全配置。因此,交换机安全是整个网络安全的重要组成部分。

1. 风暴控制

风暴控制配置过程如下。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 指定要配置的接口。

```
Switch(config)# interface interface-id
```

(3) 配置广播、多播或单播风暴控制。默认状态下,风暴控制被禁用。通常情况下,应当启用广播风暴控制。

```
Switch(config-if)# storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps
[bps-low] | pps pps [pps-low]}
```

其中各参数含义如下。

① level:指定阻塞端口的带宽上限值。当广播、多播或单播传输占到带宽的多大比例(百分比)时,端口将阻塞传输。取值范围为 0.00～100.00。如果将值设置为 100%,将不限制任何传输;如果将值设置为 0%,那么,该端口的所有广播、多播或单播都将被阻塞。建议取值范围在 30%左右。

② level-low:指定启用端口的带宽下限值。该值应当小于或等于下限值,当广播、多播或单播传输占用带宽的比例低于该值时,端口恢复转发传输。取值范围为 0.00～100.00。建议取值范围在 20%左右。

③ bps:指定端口阻塞的传输速率上限值。当广播、多播或单播传输达到每秒若干比特(bps)时,端口将阻塞传输。建议取值范围不高于端口速率的 1/3～1/2。

④ bps-low:指定端口启用的传输速率下限值。该值应当小于或等于下限值,当广播、多播或单播传输低于每秒若干比特(bps)时,端口将恢复传输。建议取值范围不高于端口速率的 1/3～1/2。如果数值较大,也可以使用 k、m 或 g 等单位表示。

⑤ pps:指定端口阻塞的转发速率上限值。当广播、多播或单播传输速率达到每秒若干包(pps)时,端口将阻塞传输。建议取值范围不高于端口转发速率的 1/3～1/2。

⑥ pps-low:指定端口启用的传输速率下限值。该值应当小于或等于下限值,当广播、多播或单播转发速率低于每秒若干包(pps)时,端口将恢复传输。建议取值范围不高于端口转发速率的 1/3～1/2。如果数值较大,也可以使用 k、m 或 g 等单位表示。

(4) 指定风暴发生时如何处理。默认状态下,将过滤外出的传输,并不发送 SNMP 陷

阱。选择 shutdown 关键字，在风暴期间将禁用端口；选择 trap 关键字，当风暴发生时，产生一个 SNMP 陷阱，向网络管理软件发出警报。通常情况下，当风暴发生时，应当选择 shutdown 关键字，从而避免风暴发生而导致的网络瘫痪。

```
Switch(config-if)# storm-control action {shutdown | trap}
```

(5) 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

(6) 显示并校验该接口当前的配置。

```
Switch# show storm-control [interface] [{broadcast | history | multicast | unicast}]
```

(7) 保存风暴控制配置。

```
Switch# copy running-config startup-config
```

使用 no storm-control {broadcast | multicast | unicast}命令，可以在指定端口禁用风暴控制功能。

提示：使用 interface range {port-range | macro macro_name}命令，可以创建端口组，从而同时配置多个端口。

2. 流控制

端口流控制配置过程如下。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 选择要配置的端口，进入接口配置模式。

```
Switch(config)# interface interface-id
```

(3) 设置端口的流控制。

```
Switch(config-if)# flowcontrol {receive | send} {on | off | desired}
```

(4) 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

(5) 显示接口状态。

```
Switch# show interfaces interface-id
```

(6) 保存配置。

```
Switch# copy running-config startup-config
```

3. 保护端口

保护端口配置过程如下。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

（2）指定要配置的接口。

```
Switch(config)# interface interface-id
```

（3）将接口配置为保护端口。

```
Switch(config-if)# switchport protected
```

（4）返回特权 EXEC 模式。

```
Switch(config-if)# end
```

（5）显示并校验该接口当前的配置。

```
Switch# show interfaces interface-id switchport
```

（6）保存配置。

```
Switch# copy running-config startup-config
```

若要禁用保护端口，可以使用 no switchport protected 接口配置命令。

注意：对于需要保证用户信息安全的环境，可以通过将用户端口设置为 Access Port，并使用该 Access Port 的 Protected Port 功能，但是这些用户有责任对自己的信息安全做出保证，即用户保证不发送 tagged 帧，交换机保证发送到 Access Port 的所有帧均为 untagged 帧。如果一个 Access Port 收到 tagged 帧，在交换机上将按照正常转发。对于一个使用了 Protected Port 功能的 Access Port，如果收到 tagged 未知名单播帧、未知名多播帧和广播帧，交换机将按照普通端口的转发规则转发给所有其他端口。

最好不要将一个 Trunk Port 设置为 Protected Port，对于使用了 Protected Port 功能的 Trunk Port，交换机对该端口收到的单播帧保证不转发给其他 Protected Port。但是对于该端口收到的 tagged 未知名多播帧、未知名单播帧和广播帧，交换机将按照普通端口的转发规则转发给所有其他端口。

4. 端口阻塞

默认状态下，未知目的 MAC 地址的广播包被允许从端口向外传输。如果未知的单播和多播通信被转发到保护端口，将导致安全问题。可以采用阻塞端口的方式，防止未知的单播和多播通信在端口间转发。

端口阻塞配置过程如下。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）指定要配置的接口。

```
Switch(config)# interface interface-id
```

（3）禁止未知多播从该端口向外传输。

```
Switch(config-if)# switchport block multicast
```

(4) 禁止未知单播从该端口向外传输。

```
Switch(config-if)# switchport block unicast
```

(5) 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

(6) 显示并校验该接口当前的配置。

```
Switch# show interfaces interface-id switchport
```

(7) 保存配置。

```
Switch# copy running-config startup-config
```

5. 端口安全

当配置端口安全时,应当注意以下问题。

① 安全端口不能是 Trunk 端口。

② 安全端口不能是 Switch Port Analyzer(SPAN)的目的端口。

③ 安全端口不能是属于 Ether Channel 的端口。

④ 安全端口不能是 Private-VLAN 端口。

⑤ 安全端口不能是一个 Aggregate 端口。

⑥ 安全端口只能是一个访问端口。

利用端口安全这个特性,可以通过限制允许访问交换机上某个端口的 MAC 地址以及 IP 地址实现严格控制对该端口的输入。当为安全端口(打开了端口安全功能的端口)配置了一些安全地址后,则除了源地址为这些安全地址的包外,这个端口将不转发其他任何包。此外,还可以限制一个端口上能包含的安全地址最大个数,如果将最大个数设置为 1,并且为该端口配置一个安全地址,则连接到这个端口的工作站(其地址为配置的安全 MAC 地址)将独享该端口的全部带宽。

为了增强安全性,可以将 MAC 地址和 IP 地址绑定起来作为安全地址。当然也可以只指定 MAC 地址而不绑定 IP 地址。

如果一个端口被配置为一个安全端口,当其安全地址的数目已经达到允许的最大个数后,如果该端口收到一个源地址不属于端口上的安全地址的包时,一个安全违例将产生。当安全违例产生时,可以选择多种方式来处理违例,比如丢弃接收到的包、发送违例通知或关闭相应端口等。

当设置了安全端口上安全地址的最大个数后,可以使用下面几种方式加满端口上的安全地址。

① 使用接口配置模式下的命令 switchport port-security mac-address mac-address [ip-address ip-address]手工配置端口的所有安全地址。

② 让该端口自动学习地址,这些自动学习到的地址将变成该端口上的安全地址,直到达到最大个数。需要注意的是,自动学习的安全地址均不会绑定 IP 地址,如果在一个端口上,已经配置了绑定 IP 地址的安全地址,则将不再通过自动学习来增加安全地址。

③ 手工配置一部分安全地址,剩下的部分让交换机自己学习。

(1) 配置安全端口

安全端口配置过程如下。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定要配置端口安全的接口。

```
Switch(config)# interface interface-id
```

③ 将接口设置为访问模式。

```
Switch(config-if)# switchport mode access
```

④ 在接口启用端口安全。

```
Switch(config-if)# switchport port-security
```

⑤ 在接口设置安全 MAC 地址的最大数量，以限制该端口所连接的计算机数量。取值范围为 1～3072，默认值是 1。如果端口只是用于连接计算机，建议采用默认值 1，以确保只有一台计算机接入。

```
Switch(config-if)# switchport port-security maximum value
```

⑥ 设置违例发生后的处理模式。当安全违例事件发生时，将端口置于 restrict 或 shutdown 模式。选择 restrict 模式时，当非法 MAC 地址或太多 MAC 连接至该接口时，将丢弃数据包，并向网管计算机发送 SNMP 陷阱通知。选择 shutdown 模式时，发生安全错误的端口将被置于 error-disable 状态，除非网络管理员使用 no shutdown 命令手工激活，否则该端口失效。为了保障网络安全起见，建议采用 shutdown 模式。

```
Switch(config-if)# switchport port-security violation {restrict | shutdown}
```

⑦ 为该接口指定安全 MAC 地址。也可以使用该命令指定最大安全 MAC 地址数。如果指定的 MAC 地址数量少于安全地址的最大数量，动态学习的 MAC 地址将被保留。如果端口只是用于连接计算机，建议为其指定安全 MAC 地址，从而有效避免其他非授权计算机的接入。

```
Switch(config-if)# switchport port-security mac-address mac-address
```

⑧ 绑定端口和 MAC 地址。

```
Switch(config-if)# switchport port-security mac-address sticky
```

⑨ 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

⑩ 查看并校验配置。

```
Switch# show port-security address interface interface-id
Switch# show port-security address
```

⑪ 保存当前配置。

```
Switch# copy running-config startup-config
```

使用 no switchport port-security mac-address mac-address 指令，可以从地址表中删除 MAC 地址。

(2) 设置端口安全老化

当为端口指定最大 MAC 地址数时，为了保障该端口能够得以充分利用，可以采用设置端口安全老化时间和模式的方式，使系统能够自动删除长时间未连接的 MAC 地址，从而不必手工删除，减少网络维护的工作量。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定要配置端口安全老化的接口。

```
Switch(config)# interface interface-id
```

③ 为安全端口设置老化时间和老化类型。老化时间的取值范围为 0～1440 分钟。采用 absolute 模式时，一旦到达指定的老化时间，那么，即将 MAC 地址从安全地址列表框中移除。采用 inactivity 时，即使到达指定的老化时间，如果没有其他数据通信，那么，MAC 地址仍然被保留在安全地址列表框中。

```
Switch(config-if)# switchport port-security [ aging time aging-time | type {absolute | inactivity} ]
```

④ 返回特权 EXEC 模式。

```
Switch(config-if)# end
```

⑤ 查看并校验配置。

```
Switch# show port security [interface interface-id] [address]
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

6. 绑定 IP 和 MAC 地址

使用下述命令，可将 MAC 地址与 IP 地址绑定在一起。

(1) 进入全局配置模式。

```
Switch# configure terminal
```

(2) 绑定 IP 地址与 MAC 地址。若要绑定若干 IP 地址，需要重复该操作。

```
Switch(config-if)# arp ip-address mac-address arpa
```

(3) 保存当前配置。

```
Switch# copy running-config startup-config
```

10.2.2 路由器安全管理

作为网络出口设备，路由器的安全对整个网络有着非常重要的影响，因此，路由器的安全应当得到更多的重视。由于 Cisco 交换机与路由器都采用相同的 Cisco IOS 操作系统，因

此，应用于路由器的许多功能和配置命令（如 IP 访问列表、时间访问列表等），也同样适用于三层交换机。

1. IP 访问列表

1）创建标准访问列表

创建标准访问列表的步骤如下。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）使用源地址或通配符定义标准 IP 访问列表。

```
Switch(config)# access-list access-list-number {deny | permit} source [source-wildcard]
```

其中各参数的含义如下。

① access-list-number：ACL 号。ACL 号相同的所有 ACL 形成一个组。在判断一个包时，使用同一组中的条目从上到下逐一进行判断，一旦遇到满足条件的条目就终止对该包的判断。1～99 或 1300～1999 为标准的 IP ACL 号。

② deny | permit：当条件匹配时，是允许包通过，还是将包丢弃。

③ source：源地址。发送包的网络或主机地址，使用点分十进制表示。当表示一组主机时，使用通配符屏蔽码。

④ source-wildcard：通配符屏蔽码。Cisco 访问列表所支持的通配符屏蔽码与子网掩码的方式是相反的。也就是说，二进制“0”表示一个匹配条件，“1”表示一个不关心条件。

any 表示任何主机。源地址和源通配符 0.0.0.0 255.255.255.255 的缩写，例如，若要拒绝从源地址 192.168.1.100 发出的报文，但允许发自其他源地址的报文，应当使用下述语句。

```
Access-list 1 deny host 192.168.1.100
Access-list 1 permit any
```

需要注意这两条语句的顺序。访问列表语句的处理是由上至下的。如果将两个语句顺序颠倒，将 permit 语句放在 deny 语句前面，则不能过滤来自主机的报文，因为 permit 语句将允许所有报文通过。访问列表中的语句顺序非常重要，不合理的语句顺序将会在网络中产生安全漏洞，或者使得用户不能很好地利用公司的网络策略。

host 表示一台主机，是源地址和源通配符 0.0.0.0 的缩写，例如，若要允许从 192.168.1.200 发出的报文，则应当使用下述语句。

```
Access-list 1 permit 192.168.1.200 0.0.0.0
```

上述语句也可以使用下面的语句代替。

```
Access-list 1 permit host 192.168.1.200
```

（3）返回特权配置模式。

```
Switch(config)# end
```

（4）校验当前设置。

```
Switch# show access-lists number
```

（5）保存当前配置。

```
Switch# copy running-config startup-config
```

使用 no access-list access-list-number 全局配置命令，可以删除全部访问列表。需要注意的是，不能从指定的访问列表中删除某个 ACE。

2）创建扩展访问列表

标准 IP 访问列表只能控制源 IP 地址，不能控制到端口。若要控制企业用户的网络应用，就需要使用扩展 IP 访问列表。

（1）进入全局配置模式。

```
Switch# configure terminal
```

（2）定义扩展 IP 访问列表，取值范围为 100～199 或 2000～2699。

```
Switch(config)# access-list access-list-number {deny | permit} protocol source source-wildcard [operator port] destination destination-wildcard [operator port]
```

或

```
access-list access-list-number {deny | permit} protocol any [operator port] any [operator port]
```

或

```
access-list access-list-number {deny | permit} protocol host source [operator port] host destination [operator port]
```

各参数的含义如下。

① protocol：要过滤的协议，例如 IP、TCP、UDP 和 ICMP 等。默认过滤所有协议，若要根据特殊协议进行报文过滤，需指定协议。

② destination destination-wildcard：目的地址和通配符屏蔽码。

③ operator：端口操作符，在协议类型为 TCP 或 UDP 时支持端口比较，支持的比较操作有：等于(eq)、大于(gt)、小于(lt)、不等于(neq)或介于(range)。如果操作符为 range，则后面需要跟两个端口。

④ port：端口号，可以用几种不同方法指定。可以显式地指定，数字或使用一个可识别的助记符，例如，可以使用 80 或 http 指定超文本传输协议，使用 21 或 ftp 指定文件传输协议。例如，若要允许来自任何地址的包含有 SMTP 数据的报文到达 192.168.10.10 主机，可以在访问列表中添加下述语句。

```
Access-list 101 permit tcp any host 192.168.10.10 eq smtp
```

（3）返回特权配置模式。

```
Switch(config)# end
```

（4）校验当前设置。

```
Switch# show access-lists number
```

（5）保存当前配置。

```
Switch# copy running-config startup-config
```

3）创建 IP 访问列表名称

命名 IP 访问列表有两个主要优点，一是可以解决 ACL 号码不足的问题；二是可以自由的删除 ACL 中的一条语句，而不必删除整个 ACL。而其主要的不足之处在于无法实现在任意位置加入新的 ACL 条目。

（1）创建标准 IP 访问控制列表名称

① 进入全局配置模式。

```
Switch# configure terminal
```

② 利用名称定义标准 IP 访问控制列表，进入访问列表配置模式。名称可以是 1～99。

```
Switch(config)# ip access-list standard name
```

③ 定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
Switch(config-std-nacl)# deny {source [source-wildcard] | host source | any}
```

或

```
Switch(config-std-nacl)# permit {source [source-wildcard] | host source | any}
```

④ 返回特权配置模式。

```
Switch(config-std-nacl)# end
```

⑤ 校验当前设置。

```
Switch# show access-lists name
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

下例显示如何创建一条 IP Standard Access-list，该 ACL 名字为 deny-host192.168.12.x。有两条 ACE，第一条 ACE 拒绝来自 192.168.12.0 网段的任一主机；第二条 ACE 允许其他任意主机。

```
Switch(config)# ip access-list standard deny-host192.168.12.x
Switch(config-std-nacl)# deny 192.168.12.0 0.0.0.255 any
Switch(config-std-nacl)# permit any
Switch(config-std-nacl)# end
Switch # show access-list
```

（2）创建扩展 IP 访问控制列表名称

① 进入全局配置模式。

```
Switch# configure terminal
```

② 利用名称定义扩展 IP 访问控制列表，进入访问列表配置模式。名称可以是 100～199。

```
Switch(config)# ip access-list extended name
```

③ 定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
Switch(config-ext-nacl)# {deny | permit} protocol {source [source-wildcard] | host source | any}
{destination [destination-wildcard] | host destination | any}
```

④ 返回特权配置模式。

```
Switch(config-std-nacl)# end
```

⑤ 校验当前设置。

```
Switch# show access-lists name
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

下例显示如何创建一条 Extended IP ACL，该 ACL 有一条 ACE，用于允许指定网络(192.168.x.x)的所有主机以 HTTP 访问服务器 172.168.12.3，但拒绝其他所有主机使用网络。

```
Switch(config)# ip access-list extended allow_0xc0a800_to_172.168.12.3
Switch(config-std-nacl)# permit tcp 192.168.0.0 0.0.255.255 host 172.168.12.3 eq www
Switch(config-std-nacl)#end
Switch # show access-list
```

例如，借助扩展 IP 访问列表，可以在 VLAN 或端口上阻止蠕虫端口，从而避免蠕虫在网络中的蔓延，保证网络的传输效率。

```
access-list 110 deny    tcp any any rang 135 139
access-list 110 deny    tcp any any eq 445
access-list 110 deny    tcp any any eq 593
access-list 110 deny    tcp any any eq 1029
access-list 110 deny    tcp any any eq 4444
access-list 110 deny    tcp any any eq 5000
access-list 110 deny    tcp any any eq 5554
access-list 110 deny    tcp any any eq 7955
access-list 110 deny    udp any any rang 135 139
access-list 110 deny    udp any any eq tftp
access-list 110 deny    udp any any range 995 999
access-list 110 deny    udp any any eq 1434
access-list 110 deny    tcp any any gt 8090
access-list 110 deny    udp any any eq 8090
access-list 110 permit ip any any
```

然后，再将该访问列表应用至端口或 VLAN，在入和出双向上启用该列表。

```
ip access-group 110 in
ip access-group 110 out
```

下例显示如何将 access-list deny_unknow_device 应用于 10/100Mbps 接口 2 上。

```
Switch(config)# interface FastEthernet 0/2
Switch (config-if)# ip access-list deny_unknow_device in
```

下例显示如何将 access-list accept_00d0f8xxxxxx_only 应用于 Gigabit 接口 2 上。

```
Switch(config)# interface GigabitEthernet 2/1
Switch (config-if)# mac access-list accept_00d0f8xxxxxx_only in
```

由于只能将一条 ACL 应用到一个接口上，因此不可能同时将类型为 IP Standard Access-list、IP Extended Access-list、MAC Extended Access-list 的 ACL 应用到某一个接口上。当将不同类型的 ACL 应用到某一个接口上时，前一个应用的 ACL 将被后一个应用的 ACL 所替换。

2. MAC 访问列表

在 VLAN 或二层接口上，可以使用 MAC 地址和 MAC 扩展 ACL 名称过滤非 IP 地址通信，从而保障企业网络访问安全，拒绝非授权用户对敏感部门的访问。配置过程与其他扩展名称 ACL 相似。

(1) 创建端口扩展访问列表名称

创建端口扩展访问列表名称的步骤如下。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 为扩展 MAC 地址列表定义一个名称，进入扩展 MAC 地址列表配置模式。

```
Switch(config)# mac access-list extended name
```

③ 定义允许或拒绝的源 MAC 地址或目的 MAC 地址。使用 host，可以指定特定主机的 MAC 地址；使用掩码，可以指定多个主机的 MAC 地址。

```
Switch (config-ext-mac)# {deny | permit} {any | host source MAC address | source MAC address
mask} {any | host destination MAC address | destination MAC address mask}
```

④ 返回特权配置模式。

```
Switch(config-ext-mac)# end
```

⑤ 校验当前设置。

```
Switch# show access-lists name
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

(2) 将端口访问列表应用到二层接口

将端口访问列表应用到二层接口的步骤如下。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 指定要应用该 IP 访问列表的二层接口。

```
Switch(config)#interface interface-id
```

③ 将 MAC 访问列表应用到二层接口。注意，该命令不适用于 Ether Channel。

```
Switch(config-if)# mac access-group {name} {in}
```

④ 返回特权配置模式。

```
Switch(config-if)# end
```

⑤ 校验当前设置。

```
Switch# show mac access-group [interface interface-id]
```

⑥ 保存当前配置。

```
Switch# copy running-config startup-config
```

下例显示如何创建及显示一条 MAC Extended ACL，以名字 macext 命名。该 MAC 扩展 ACL 拒绝所有符合指定源 MAC 地址的 aarp 报文。

```
Switch(config)# mac access-list extended macext
Switch(config-ext-macl)# deny host 00d0.f800.0000 any aarp
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists macext
Extended MAC access list macext
deny host 00d0.f800.0000 any aarp
permit any any
```

3. 创建并应用 VLAN 访问列表

（1）创建 VLAN 访问列表

创建 VLAN 访问列表的步骤如下。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 创建 VLAN 映射，并给该 VLAN 访问列表定义一个名称和序号，进入 VLAN 访问列表配置模式。

```
Switch(config)# vlan access-map name [number]
```

③ 为 VLAN 映射设置动作，默认为转发(forward)。

```
Switch (config-access-map)# action {drop | forward}
```

④ 借助一个或多个标准或扩展访问列表匹配包(使用 IP 或 MAC 地址)。IP 包只能被标准或扩展 IP 访问列表匹配；非 IP 包只能被 MAC 扩展访问列表匹配。

```
Switch (config-access-map)# match {ip | mac} address {name | number} [name | number]
```

⑤ 返回特权配置模式。

```
Switch(config-access-map)# end
```

⑥ 校验当前设置。

```
Switch# show running-config
```

⑦ 保存当前配置。

```
Switch# copy running-config startup-config
```

(2) 将 VLAN 访问列表应用到 VLAN

将 VLAN 访问列表应用到 VLAN 的步骤如下。

① 进入全局配置模式。

```
Switch# configure terminal
```

② 将 VLAN 映射应用至一个或多个 VLAN。可以使用“-”或“,”指定若干 VLAN。

```
Switch(config)# vlan filter mapname vlan-list list
```

③ 返回特权配置模式。

```
Switch(config-access-map)# end
```

④ 校验当前设置。

```
Switch# show running-config
```

⑤ 保存当前配置。

```
Switch# copy running-config startup-config
```

4. 静态地址转换的实现

所谓静态地址转换是指将合法 IP 地址一一对应地转换为内部私有 IP 地址。如果企业网络获得多个合法 IP 地址,可以借助静态地址转换方式,将合法 IP 地址转换为内部服务器的 IP 地址,从而实现对企业网络和 Internet 对服务器的访问。

例如,内部网络使用的 IP 地址段为 192.168.100.1～192.168.100.62,路由器局域网端口(即默认网关)的 IP 地址为 192.168.100.1,子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 121.17.46.128～121.17.46.135,路由器广域网中的 IP 地址为 121.17.46.129,子网掩码为 255.255.255.248,可用于转换的 IP 地址为 121.17.46.133。要求将内部网址 192.168.100.2～192.168.100.6 分别转换为合法 IP 地址 121.17.46.130～121.17.46.134。

(1) 设置外部端口。

```
interface serial 0/0
ip address 121.17.46.133 255.255.255.248
ip nat outside
```

(2) 设置内部端口。

```
interface fastethernet 0/0
ip address 192.168.100.1 255.255.255.192
ip nat inside
```

(3) 在内部本地地址与内部合法地址之间建立静态地址转换。

ip nat inside source static 内部本地地址 内部合法地址

示例：

```
ip nat inside source static 192.168.100.2 121.17.46.130
!--将内部网络地址 192.168.100.2 转换为合法 IP 地址 121.17.46.130
ip nat inside source static 192.168.100.3 121.17.46.131
!--将内部网络地址 192.168.100.3 转换为合法 IP 地址 121.17.46.131
ip nat inside source static 192.168.100.4 121.17.46.132
!--将内部网络地址 192.168.100.4 转换为合法 IP 地址 121.17.46.132
ip nat inside source static 192.168.100.5 121.17.46.133
!--将内部网络地址 192.168.100.5 转换为合法 IP 地址 121.17.46.133
ip nat inside source static 192.168.100.6 121.17.46.134
!--将内部网络地址 192.168.100.6 转换为合法 IP 地址 121.17.46.134
```

至此，静态地址转换配置完毕。

5. 动态地址转换的实现

所谓动态地址转换是指将内部私有 IP 地址动态地转换为合法 IP 地址池内的 IP 地址，对应关系是不固定的。如果企业网络获得多个合法 IP 地址，可以借助动态地址转换方式，实现 Internet 连接共享。

例如，内部网络使用的 IP 地址段为 172.16.100.1～172.16.100.254，路由器局域网端口(即默认网关)的 IP 地址为 172.16.100.1，子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 121.17.46.128～121.17.46.191，路由器广域网中的 IP 地址为 121.17.46.129，子网掩码为 255.255.255.192，可用于转换的 IP 地址范围为 121.17.46.130～121.17.46.190。要求将内部网址 172.16.100.1～172.16.100.254 动态转换为合法 IP 地址 121.17.46.130～121.17.46.190。

(1) 设置外部端口。

设置外部端口命令的语法如下。

ip nat outside

示例：

```
interface serial 0/0
!--进入串行端口 serial 0/0
ip address 121.17.46.129 255.255.255.248
!--将其 IP 地址指定为 121.17.46.129,子网掩码为 255.255.255.248
ip nat outside
!--将串行口 serial 0/0 设置为外部端口
!--注意,可以定义多个外部端口
```

(2) 设置内部端口。

设置内部端口命令的语法如下。

ip nat inside

示例：

```
interface fastethernet 0/0
!--进入快速以太网端口 fastethernet 0/0
ip address 172.16.100.1 255.255.255.0
```

```
!--将其 IP 地址指定为 172.16.100.1,子网掩码为 255.255.255.0
ip nat inside
!--将 fastethernet 0/0 设置为内部端口
!--注意,可以定义多个内部端口
```

(3) 定义合法 IP 地址池。

定义合法 IP 地址池命令的语法如下。

```
ip nat pool 地址池名称 起始 IP 地址 终止 IP 地址 子网掩码
```

其中,地址池名字可以任意设定。

示例:

```
ip nat pool chinanet 121.17.46.130 121.17.46.190 netmask 255.255.255.192
!--指明地址缓冲池的名称为 chinanet,IP 地址范围为 121.17.46.130~121.17.46.190
!--子网掩码为 255.255.255.192.需要注意的是,即使掩码为 255.255.255.0,也会由起始 IP 地址和
终止 IP 地址对 IP 地址池进行限制
!--或 ip nat pool test 121.17.46.130 121.17.46.190 prefix-length 26
```

(4) 定义内部网络中允许访问 Internet 的访问列表。

定义内部访问列表命令的语法如下。

access-list 标号 permit 源地址 通配符

其中,标号为 1~99 之间的整数。

示例:

```
access-list 1 permit 172.16.100.0 0.0.0.255
!--允许访问 Internet 的网段为 172.16.100.0~172.16.100.255,主机掩码为 0.0.0.255
```

需要注意的是,在这里采用的是主机掩码,而非子网掩码。子网掩码与主机掩码的关系为:主机掩码+子网掩码=255.255.255.255,例如,子网掩码为 255.255.0.0,则主机掩码为 0.0.255.255;子网掩码为 255.0.0.0,则主机掩码为 0.255.255.255;子网掩码为 255.255.0.0,则主机掩码为 0.3.255.255;子网掩码为 255.255.255.192,则主机掩码为 0.0.0.63。

另外,如果想将多个 IP 地址段转换为合法 IP 地址,可以添加多个访问列表,例如,当欲将 172.16.98.0~172.16.98.255 和 172.16.99.0~172.16.99.255 转换为合法 IP 地址时,应当添加下述命令。

```
access-list 2 permit 172.16.98.0 0.0.0.255
access-list 2 permit 172.16.99.0 0.0.0.255
```

(5) 实现网络地址转换。

在全局设置模式下,将由 access-list 指定的内部本地地址与指定的内部合法地址池进行地址转换。命令语法如下。

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字
```

示例:

```
ip nat inside source list 1 pool chinanet
```

如果有多个内部访问列表,可以一一添加,以实现网络地址转换。

示例:

```
ip nat inside source list 2 pool chinanet
ip nat inside source list 2 pool chinanet
```

至此,动态地址转换设置完毕。

10.3 网络安全设备管理

无论是大中型企业网络,还是小型家庭办公网络,对网络安全方面的要求一直保持上升趋势。解决网络安全问题最常用的防护手段就是安装相应的安全设备,尤其是对于大中型规模的网络而言,网络安全设备更是实现网络安全必不可少的装备。网络安全设备目前主要包括 4 种类型,即防火墙、IDS、IPS 和漏洞扫描器,在当前网络中主要使用的是防火墙。

10.3.1 网络安全设备概述

防火墙(Fire Wall)是目前最重要的一种网络防护设备。网络防火墙的主要功能就是抵御外来非法用户的入侵,就像是矗立在内部网络和外部网络之间的一道安全屏障。外部网络用户的访问必须先经过安全策略过滤,而内部网络用户对外部网络的访问则无须过滤。这些过滤策略就是防火墙工作的主要依据。另外,网络防火墙还具有隔离网段、提供代理服务和流量控制等功能,可以满足用户的各种需求。图 10-1 所示为 Cisco ASA 5510 防火墙。

防火墙的主要功能有以下几个方面。

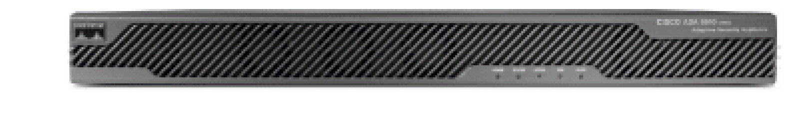


图 10-1 Cisco ASA 5510

(1) 创建一个阻塞点

防火墙在内部网络和外部网络之间建立一个检查点,这就要求所有的数据包都要通过这个检查点。一旦这些检查点建立,防火墙设备就可以监视、过滤和检查所有进来和出去的流量,网络安全产业称这些检查点为“阻塞点”。通过强制所有进出流量都通过这些检查点,网络管理员可以集中在较少地方来实现安全目的。如果没有这样一个供监视和控制信息的点,系统或安全管理员则要在大量的地方来进行监测,其实这个检查点也就是网络边界。

(2) 隔离不同的网络

防火墙最基本的功能就是隔离内外网络,不仅确保不让非法用户入侵,更要保证内部信息的不外泄。非法用户的入侵主要是通过获取对方的用户名和密码,以及其他一些重要的信息来实现的,企业网络的内部数据更是黑客觊觎已久的“肥肉”。内部网络中不被人注意的一个细节可能包含了有关安全的线索,从而为攻击者留下可乘之机。使用防火墙则可以屏蔽这些内部细节,如 Finger 和 DNS 等服务。Finger 服务可以显示主机的所有用户的注册名、真名、最后登录时间和使用 Shell 类型等,Finger 显示的信息非常容易被攻击者截获。攻击者通过所获取的信息可以知道一个系统使用的频繁程度,这个系统是否有用户正在连线上网等信息。

(3) 强化网络安全策略

通过以防火墙为中心的安全方案配置,能将所有安全软件(如密码、加密、身份证和审计等)设置在防火墙上。这比将网络安全分散到每个主机上,管理更集中而且更经济。各种安全措施的有机结合,更能有效地对网络安全性能起到加强作用。

(4) 包过滤

包过滤是所有防火墙都具有的基本功能。由最初的 IP 地址、端口判定控制,到今天的判断通信报文协议头的各部分,以及通信协议的应用层命令、内容、用户认证、用户规则甚至状态检测等,无不标志着包过滤的进步。特别是状态监测技术,可以支持多种协议和应用程序,并可以很容易地实现应用层的扩充。它在现有协议栈中加载一个检测模块,模块在网络层截取数据包,然后在所有的通信层上抽取有关的状态信息,根据该状态位判断该通信是否符合安全策略。

(5) 网络地址转换

网络地址转换(Network Address Translation,NAT)功能似乎已经成了防火墙的"隐身术",绝大多数防火墙都加入了该功能。目前防火墙一般采用双向 NAT:SNAT 和 DNAT。SNAT 用于对内部网络地址进行转换,对外部网络隐藏内部网络的结构,使得对内部的攻击更加困难,并可以节省 IP 资源,有利于降低成本。而 DNAT 主要实现外网主机对内网和 DMZ 区主机的访问。

(6) 流量控制和统计分析

流量控制可以分为基于 IP 地址的控制和基于用户的控制。基于 IP 地址的控制是对通过防火墙各个网络接口的流量进行控制。基于用户的控制是通过用户登录来控制每个用户的流量,从而防止某些应用或用户占用过多的资源。并且通过流量控制可以保证重要用户和重要接口的连接。流量统计是建立在流量控制基础之上的。一般防火墙通过对基于 IP、服务、时间和协议等的数据进行统计,并可以与管理界面实现挂接,实时或者以统计报表的形式输出结果。

(7) URL 级信息过滤

它是代理模块常常实现的一部分,很多厂家把这个功能单独提取出来,它其实是和代理模块一起实现的。URL 过滤用来控制内部网络对某些站点的访问,如禁止访问某些站点、禁止访问站点下的某些目录、只允许访问某些站点或者其下面的文件和目录等。

10.3.2 Cisco ASDM 配置

Cisco 自适应安全设备管理器(Adaptive Security Device Manager,ASDM)通过一个直观、易用、基于 Web 的管理界面,提供了世界级的安全管理和监控服务。结合 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备,Cisco ASDM 提供的智能向导、强大的管理工具和灵活的监控服务,进一步增强 Cisco 安全设备套件提供的先进的集成安全和网络功能,从而加速安全设备的部署。其基于 Web 的安全设计可使用户能随时随地访问 Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备。

1. Cisco ASDM 简介

作为自适应安全设备管理器,Cisco ASDM(如图 10-2 所示)以图形界面方式,配置和管理 Cisco PIX 和 Cisco ASA 安全设备。

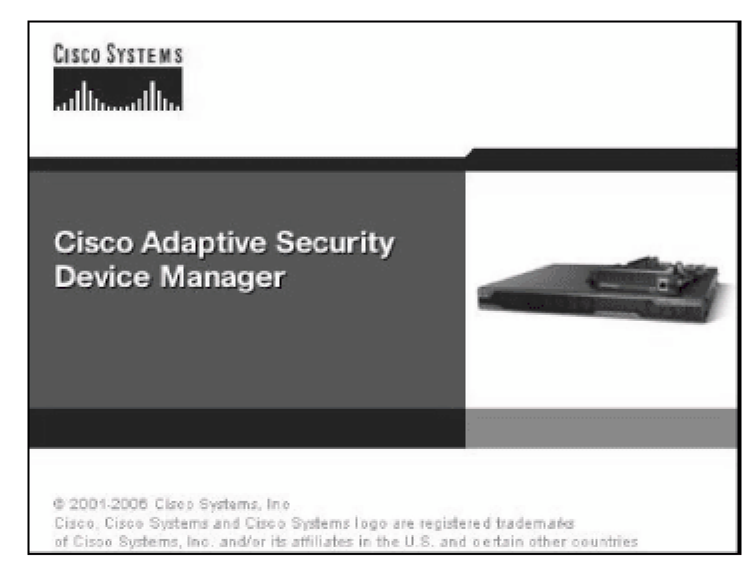


图 10-2 Cisco ASDM

Cisco ASDM 具有如下特点。

(1) 集成化管理提高管理效率

网络上任何支持 Java 插件的计算机,都可以借助 Web 浏览器访问 Cisco ASDM,使安全管理员能迅速、

安全地访问自己的 Cisco ASA 和 Cisco PIX 设备。为管理员提供了基于 Windows 的全新配置方式，管理员可从单一管理工作站连接多个安全设备，从而提高了配置和管理安全设备的效率。

（2）启动向导加速安全设备的部署

Cisco ASDM 拥有一个启动向导，加速了安全设备部署流程。一系列简单的渐进式配置界面，可帮助管理员快速启动和运行设备，创建使流量能安全地在网络中传输的稳固配置。该启动向导能配置多种可选特性，如动态主机控制协议（DHCP）服务器设置、网络地址转换（NAT）、管理员访问和自动更新。自动更新是一个具革命性意义的远程管理功能，可确保设备配置和软件镜像保持最新状态。

（3）仪表盘提供重要实时系统状态信息

Cisco ASDM 拥有一个动态仪表盘，提供全面的系统概述和设备状态统计数据概览。可自动检测所配置的 Cisco 安全设备，并显示每个设备的软件版本、许可信息和重要统计数据。在复杂的网络环境中，不仅为管理员提供了实时状态指示灯，还为强大的分析工具和高级监控功能提供了启动点。其实时系统日志浏览器，具有模式匹配功能，可根据网络地址、端口号、主机名等过滤系统日志。此外，还提供了一个强大的搜索引擎，可帮助管理员确定在何处配置特定特性，只需单击鼠标即可方便地获得搜索结果。

（4）安全策略管理降低运营成本

Cisco ASDM 强大的管理服务功能，简化了安全策略定义和持续策略维护，使安全管理员能创建可重复使用的网络和服务对象组，以及可实施多项安全策略的策略检测图。支持范围广泛的访问控制功能，如基于用户和用户组的访问列表、基于时间的访问列表，以及进/出访问列表。管理员可根据不同条件划分网络流或流量级别，然后，向每个流或流量级别应用一套可定制的检测服务、服务质量（QoS）服务和连接服务。这些先进的访问控制和应用检测功能，与易用的持续策略管理服务相配合，可确保各种规模的企业都能获得强大、动态的安全设置。

（5）安全服务实现基于角色的、安全的管理访问

Cisco ASDM 集成了一系列强大的安全服务，可防止对设备进行未授权管理访问。支持多种验证管理员的方法，如 Cisco ASA 或 Cisco PIX 的本地验证数据库，或者由 RADIUS/TACACS 服务器进行验证。Cisco ASDM（运行在管理员计算机上）和安全设备间的所有通信，都通过采用 56 位数据加密标准（DES），或者更安全的 168 位三重 DES（3DES）算法的安全套接字层（SSL）加密。Cisco ASDM 支持多达 16 级可定制管理访问级别，为管理员和操作人员提供相应的许可级别，来访问所管理的每个 Cisco 安全设备（如仅限监控、只读访问配置等）。

2. 安全策略设置

FWSM/ASA/PIX 连接互联网，在只有内、外两个安全区域时，内网用户仅是单纯的上网访问，在安全策略设置上，通常包括以下几种设置。

（1）内到外全部允许，外到内全部拒绝。

（2）内到外和外到内都要做 ACL 控制、映射、NAT。

（3）设置 IPSec、12TP、SSLVPN。

当今的安全威胁需要用新的方法消除，要实现全面的应用安全性，需要提高对整个网络

中的应用的敏感性,而不是用一种方法保护网络中的所有应用。每种应用都需要一组通用服务,以及其他应用专用检测服务。这些应用检测服务必须满足当今网络的性能和服务要求,所有要求都必须与清晰、全面的架构密切相连,以便灵活地部署和实施应用安全策略。Cisco ASA 5500 系列自适应安全设备不但能提供新型应用保护方法,还能保护关键业务应用的可用性和完整性。

Cisco ASA 5500 系列通过自适应识别和防御架构,进一步提高了网络的安全性和策略控制。利用遍及所有主要网络协议的应用安全检测引擎,Cisco ASA 5500 系列允许部署全面的应用安全策略。每种检测引擎都监控应用流,并能够标示和阻止针对特定协议的非法操作。图 10-3 所示为安全策略的设置窗口。

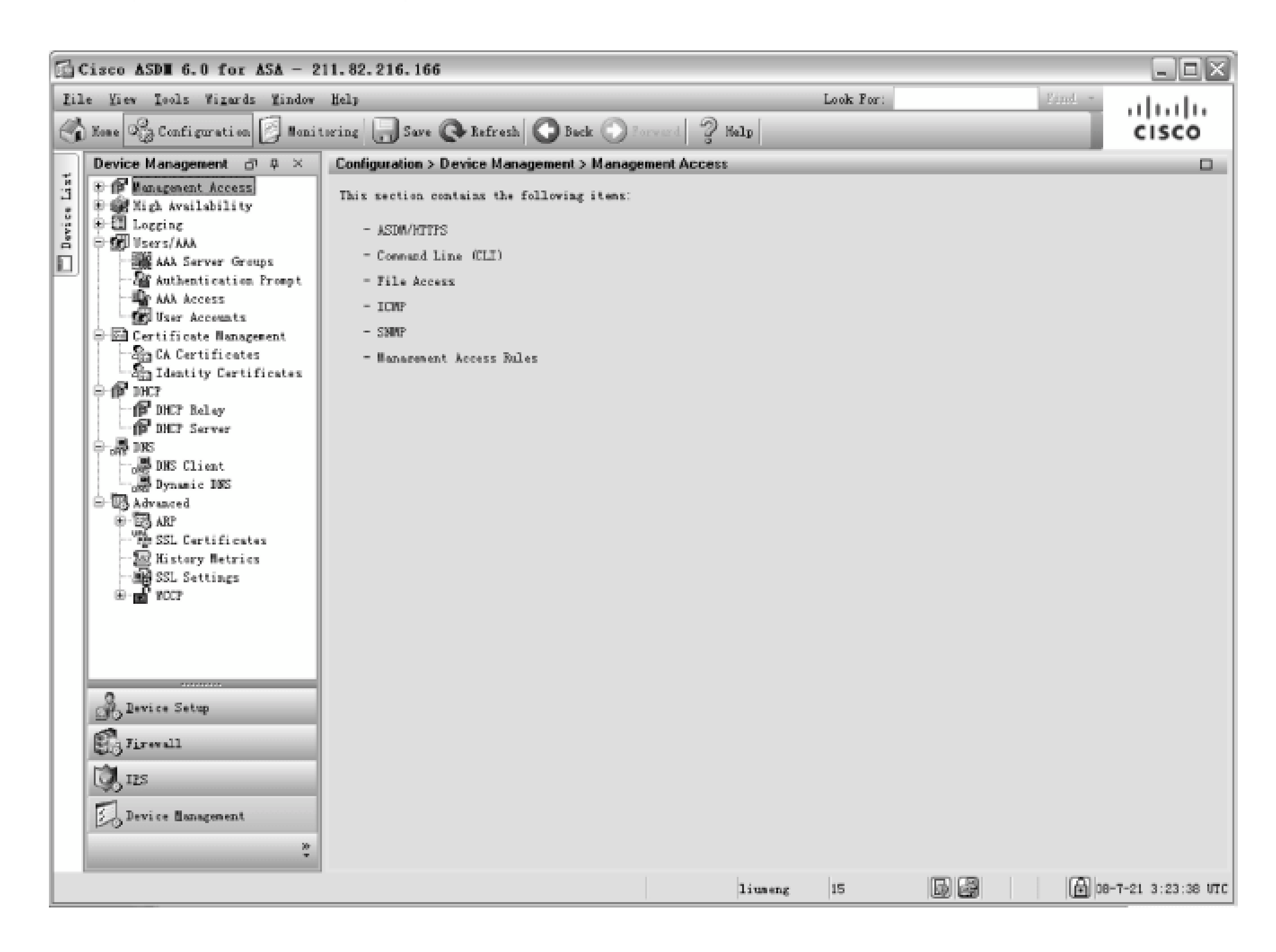


图 10-3 安全策略

3. DMZ 配置

DMZ 网络拓扑结构(如图 10-4 所示)具有如下特征。

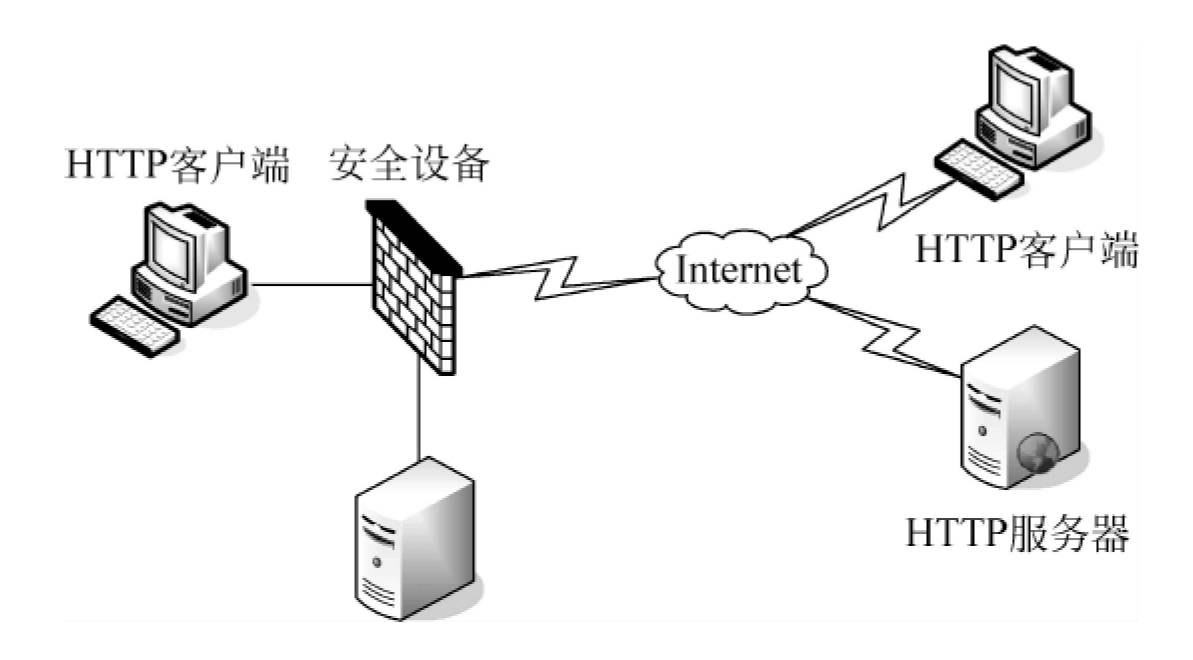


图 10-4 DMZ 拓扑结构

① Web 服务器连接至安全设备的 DMZ 接口。

② HTTP 客户端位于私有网络,可以访问位于 DMZ 中的 Web 服务器,并且可以访问 Internet 中的设备。

③ Internet 中的 HTTP 客户端允许访问 DMZ 区的 Web 服务器,除此之外的其他所有

的通信都被禁止。

④ 网络有两个可路由的 IP 地址可以被公开访问：安全设备外部端口的 IP 地址为 209.165.200.225，DMZ 中 Web 服务器的公开 IP 地址为 209.165.200.226。

(1) 运行 ASDM

运行 ASDM 的步骤如下。

① 打开 Web 浏览器，在地址栏中输入安全设备的 IP 地址：https://211.82.216.166/admin/，显示图 10-5 所示的 Cisco ASDM 6.0 对话框。

② 单击 Run ASDM 按钮，显示图 10-6 所示的 Cisco ASDM Launcher v1.5(22)程序的登录窗口。根据实际情况，输入 IP 地址、用户名和密码。

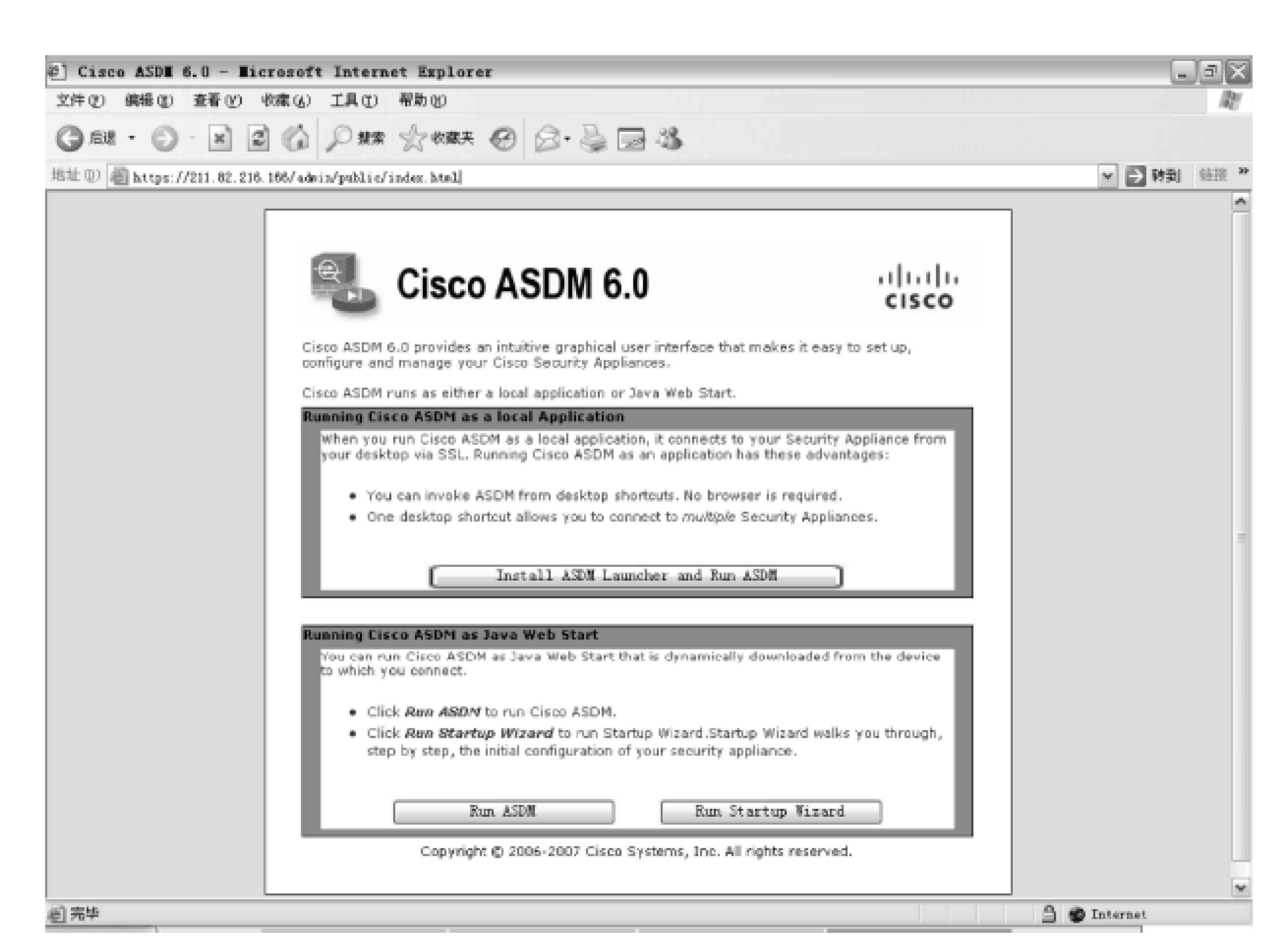




图 10-5　Cisco ASDM 6.0 对话框



图 10-6　Cisco ASDM Launcher v1.5(22)登录窗口

③ 单击 OK 按钮，显示图 10-7 所示的 Cisco ASDM 6.0 for ASA 主窗口。

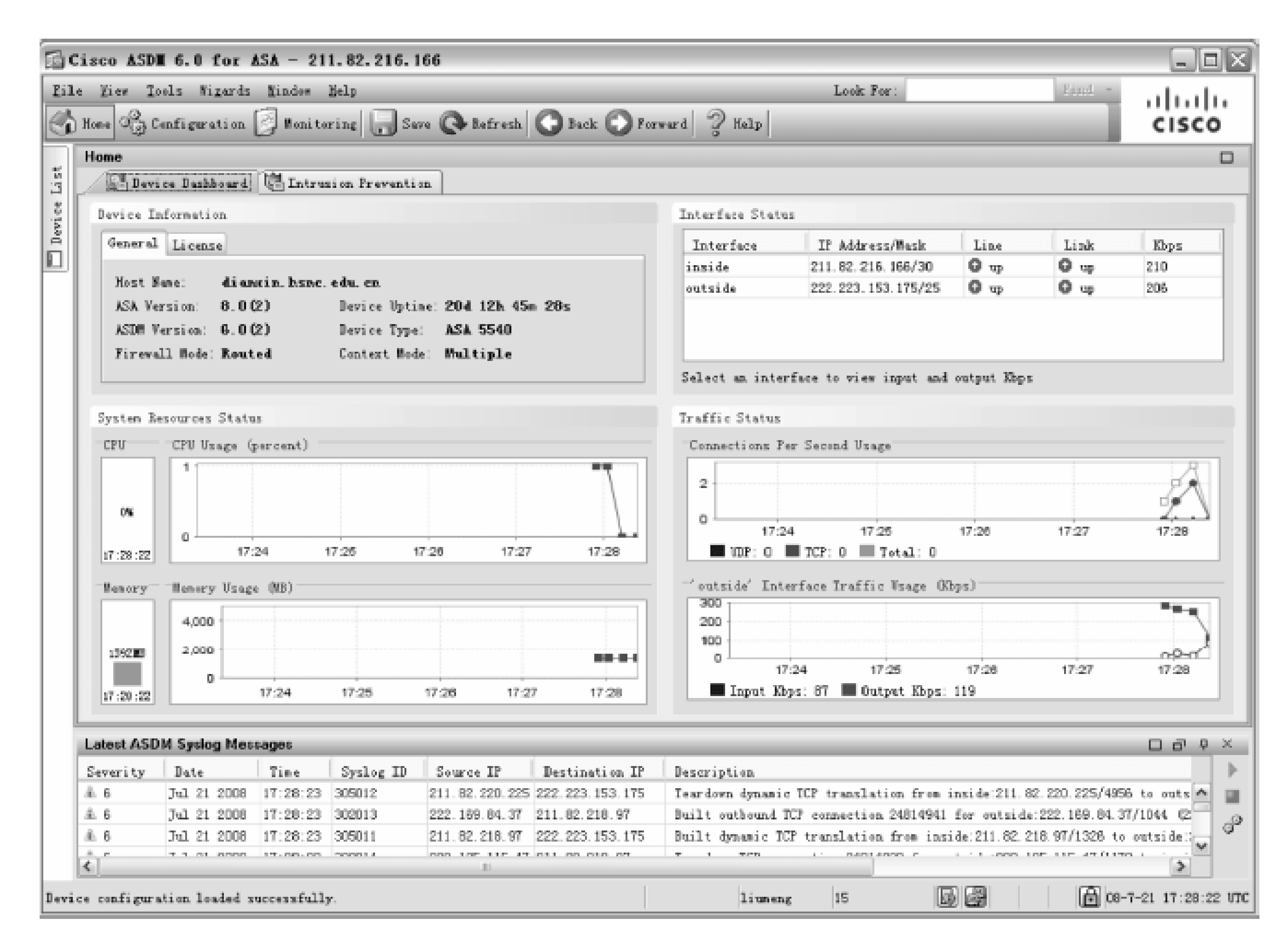


图 10-7　Cisco ASDM 6.0 for ASA 主窗口

（2）为 NAT 创建 IP 地址池

安全设备使用网络地址转换和端口地址转换防止内部 IP 地址暴露在外部网络或 Internet 中。这里介绍如何为 DMZ 接口和外部接口创建一个可以被转换的 IP 地址池。

提示：一个 IP 地址池可以同时包含 NAT 和 PAT 条目，也可以包含一个以上接口的条目。

首先指定 DMZ 的 IP 地址范围。

① 在 ASDM 窗口工具栏，单击 Configuration 图标，在左侧栏中选择 Firewall 选项区域中的 NAT Rules 规则选项，显示图 10-8 所示的窗口。

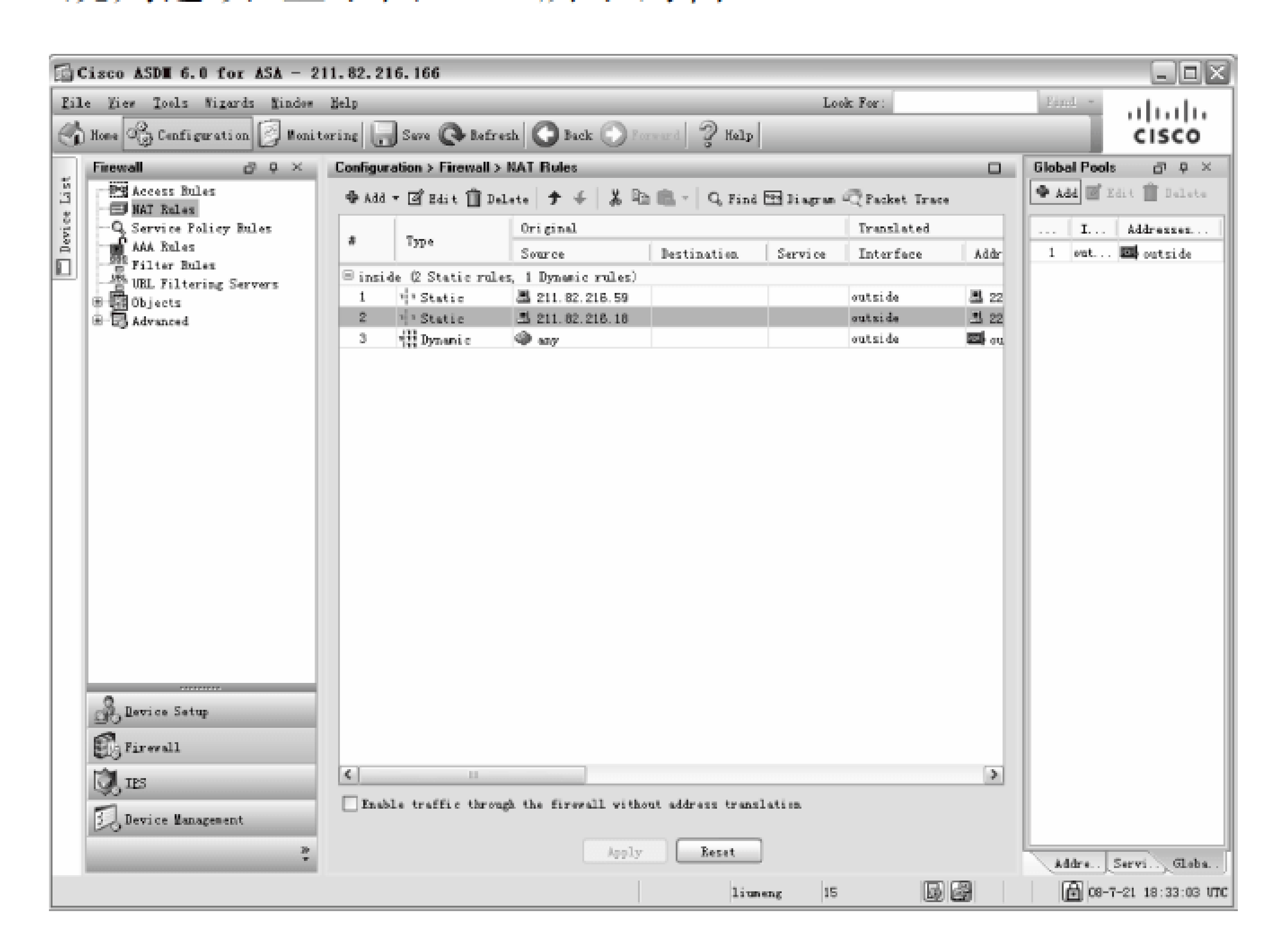


图 10-8　NAT Rules 规则

② 在右侧栏中选择 Global Pools 选项卡，单击 Add 按钮，显示图 10-9 所示的 Add Global Address Pool 对话框，为 DMZ 接口创建一个新的全局地址池。

③ 从 Interfaces 下拉列表框中，选择 DMZ 选项，在 Pool ID 文本框中输入新创建地址池的 ID 号，如 1。

④ 在 IP Addresses to Add 选项区域，指定 DMZ 接口使用的 IP 地址范围。

⑤ 单击 Add 按钮，将该 IP 地址范围添加至 Addresses Pool。

⑥ 单击 OK 按钮，返回至 NAT Rules 窗口。

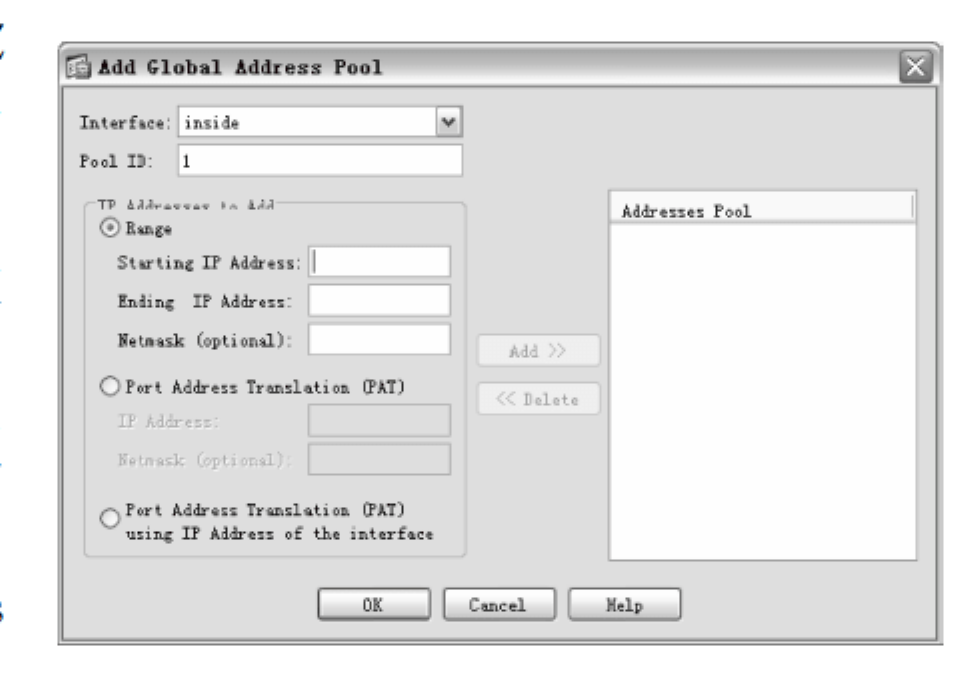


图 10-9　Add Global Address Pool 对话框

然后为外部端口指定 IP 地址池。为外部端口指定 IP 地址被用于转换私有 IP 地址，从而实现内部客户端对 Internet 的安全访问。借助 PAT 技术，可以使用同一合法 IP 地址将内部不同的服务器发布至 Internet。

① 在 NAT Rules 窗口右侧选择 Global Pools 选项卡，单击 Add 按钮，显示图 10-10 所示的 Add Global Address Pool 对话框。

② 在 Interface 下拉列表框中，选择 outside 选项，为外部接口指定地址池 ID 号，例如 2。可以将这些地址添加到与 DMZ 接口相同的 IP 地址池。

③ 选中 Port Address Translation (PAT) using IP Address of the interface 单选按钮，单击 Add 按钮将该地址添加至 Addresses Pool。

④ 单击 OK 按钮，返回 Cisco ASDM 配置窗口。确认配置无误后，在 ASDM 主窗口中，单击 Apply 按钮即可。

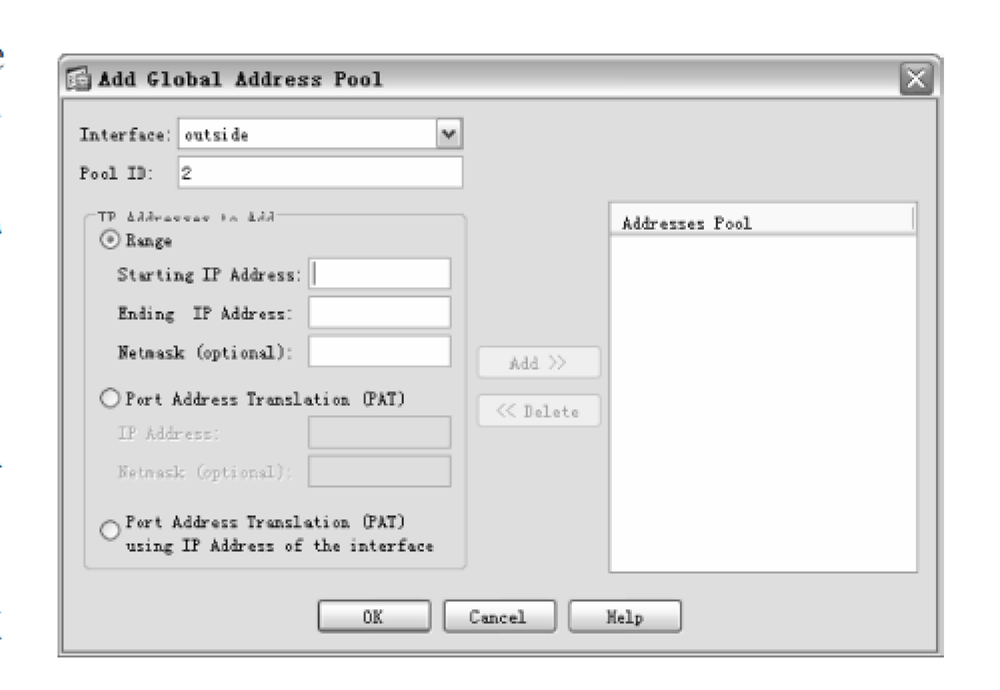


图 10-10　为外部接口指定地址池 ID 号

(3) 配置内部客户端访问 DMZ 区的 Web 服务器

在上述配置中，为内部客户端设置了安全的私有 IP 地址池，还需要配置一条 NAT 规则，用于实现内部客户端对 DMZ 区域中 Web 服务器的安全访问。

① 在 ASDM 主窗口工具栏中，单击 Configuration 图标。在左侧栏中选择 NAT Rules 选项，显示图 10-11 所示的 NAT Rules 规则窗口。

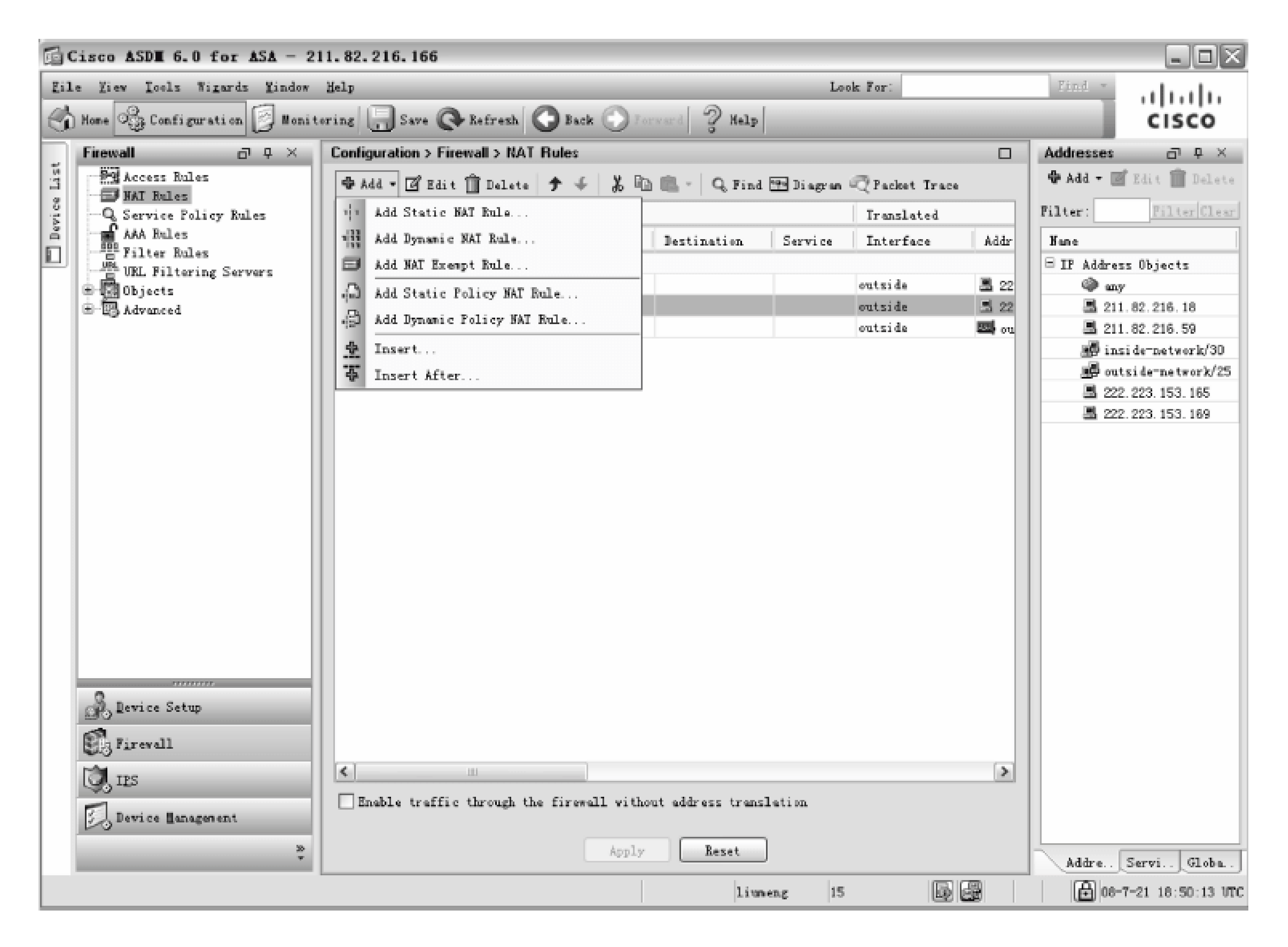


图 10-11　NAT Rules 规则窗口

② 在 Add 下拉列表框中选择 Add Dynamic NAT Rule 命令，显示图 10-12 所示的 Add Dynamic NAT Rule 对话框。

③ 在 Original 选项区域，指定被转换的 IP 地址。从 Interface 下拉列表框中，选择 inside 选项，在 Source 文本框中，输入内部客户端使用的 IP 网络号。

④ 在 Translated 选项区域，指定转换的目的 IP 地址。从 Interface 下拉列表框中，选择 DMZ 选项，指定该地址池使用动态 NAT 规则。选中 Select 复选框，选择全局地址池 ID。

提示：如果欲添加的地址池不存在，可以单击 Add 按钮创建新的 IP 地址池。

⑤ 单击 OK 按钮，添加动态 NAT 规则，并返回至 NAT Rules 窗口。ASDM 将添加两条规则，因为同一 IP 地址池同时被转换使用。

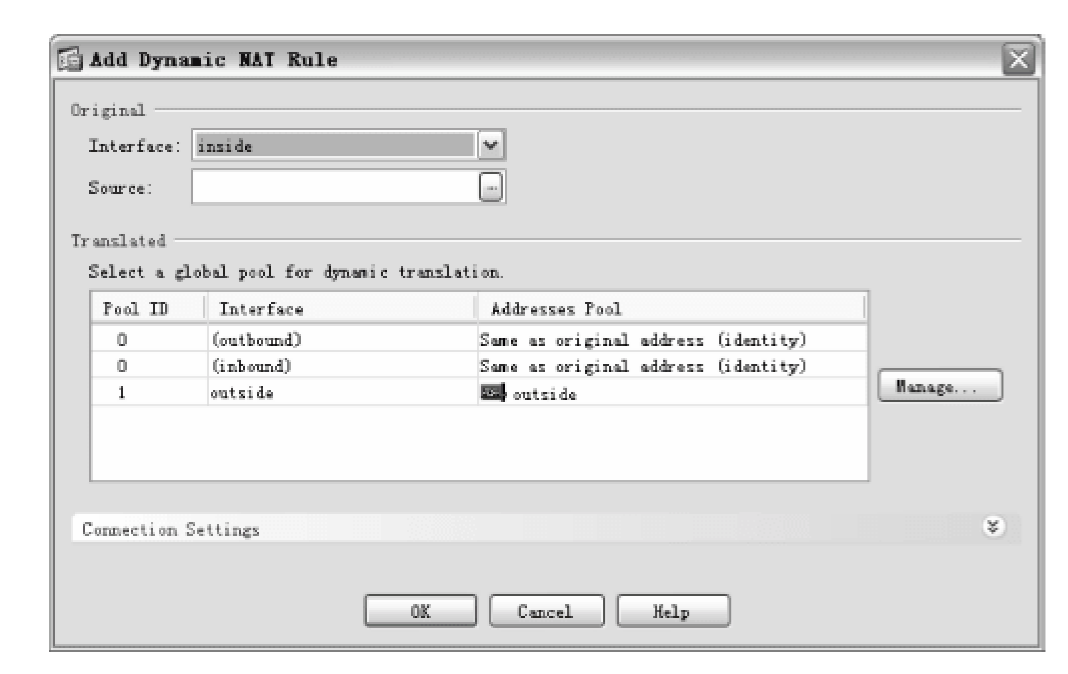


图 10-12 Add Dynamic NAT Rule 对话框

（4）配置内部客户端访问 Internet

在以上述配置中，借助 NAT 规则，可以实现内部客户端对 DMZ 区中 Web 服务器的访问。当然，借助 NAT 规则也应当能够实现内部客户端对 Internet 的访问。不过，管理员无须再创建任何规则，因为 IP 地址池包括了两种需要转换的地址，即 DMZ 接口使用的 IP 地址和外部接口使用的 IP 地址。

（5）为 Web 服务器配置外部 ID

DMZ 中的 Web 服务器需要为 Internet 中所有的主机提供访问服务。该配置需要将 DMZ 中的 Web 服务器的私有 IP 地址转换为公有 IP 地址，允许外部 HTTP 客户端实现对 Web 服务的访问。

① 在 ASDM 主窗口工具栏中，单击 Configuration 图标。在左侧栏中选择 Firewall 选项区域中的 NAT Rules 选项，从 Add 下拉列表框中，选择 Add Static NAT Rule 选项，显示图 10-13 所示的 Add Static NAT Rule 对话框。



图 10-13 Add Static NAT Rule 对话框

② 从 Original 选项区域的 Interface 下拉列表框中选择 DMZ 接口；在 Source 文本框中，输入 DMZ 区 Web 服务器的 IP 地址。

③ 在 Translated 选项区域，指定 Web 服务器使用的公有 IP 地址。从 Interface 下拉列表框中，选择 outside 选项，从 Use IP Address 下拉列表框中，选择 DMZ 区 Web 服务器使用的公有 IP 地址。

④ 单击 OK 按钮，添加规则并返回 NAT Rules 窗口。

⑤ 单击 Apply 按钮，保存安全配置的修改。

（6）允许 Internet 用户访问 DMZ 的 Web 服务

默认情况下，安全设备禁止来自公共网络的所有通信。因此，必须创建一个安全规则，允许来自 Internet 用户对 DMZ 区中 Web 服务器的访问，即允许来源于 Internet 任意用户的针对 DMZ 中 Web 服务器的流入和流出的 HTTP 通信。

① 在 ASDM 主窗口工具栏中，单击 Configuration 图标。在左侧栏中选择 Security Policy 选项，从 Add 下拉列表框中，选择 Add Access Rule 选项，显示图 10-14 所示的 Add Access Rule 对话框。

② 在 Interface 下拉列表框中选择 outside 选项；在 Action 选项区域中，选中 Permit 单选按钮。

③ 在 Source 下拉列表框中，设置允许发起访问的源 IP 地址，单击 按钮，显示图 10-15 所示的 Browse Source 对话框。

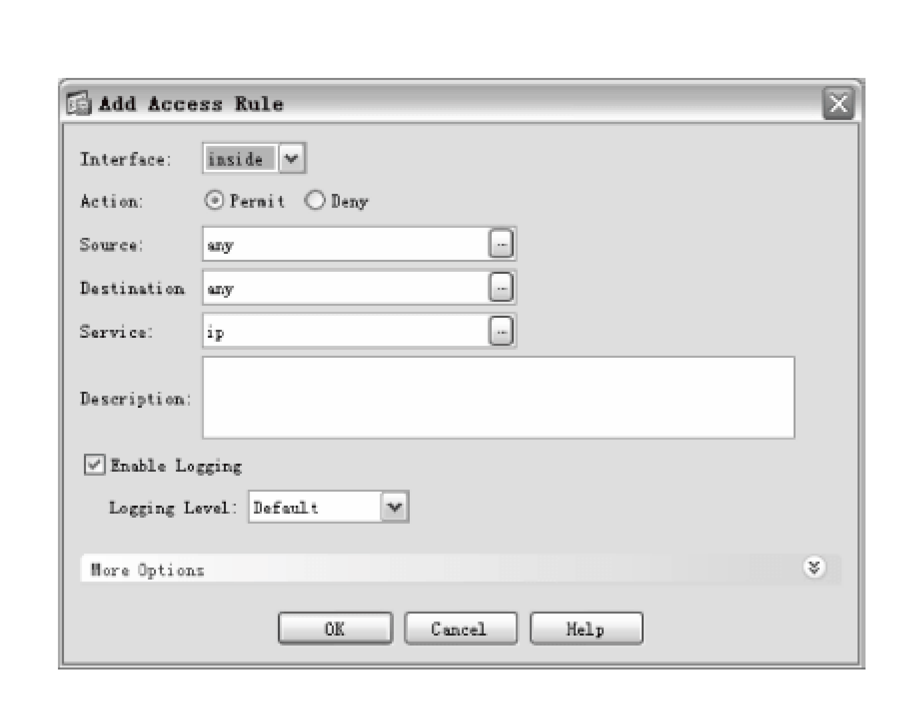




图 10-14　Add Access Rule 对话框

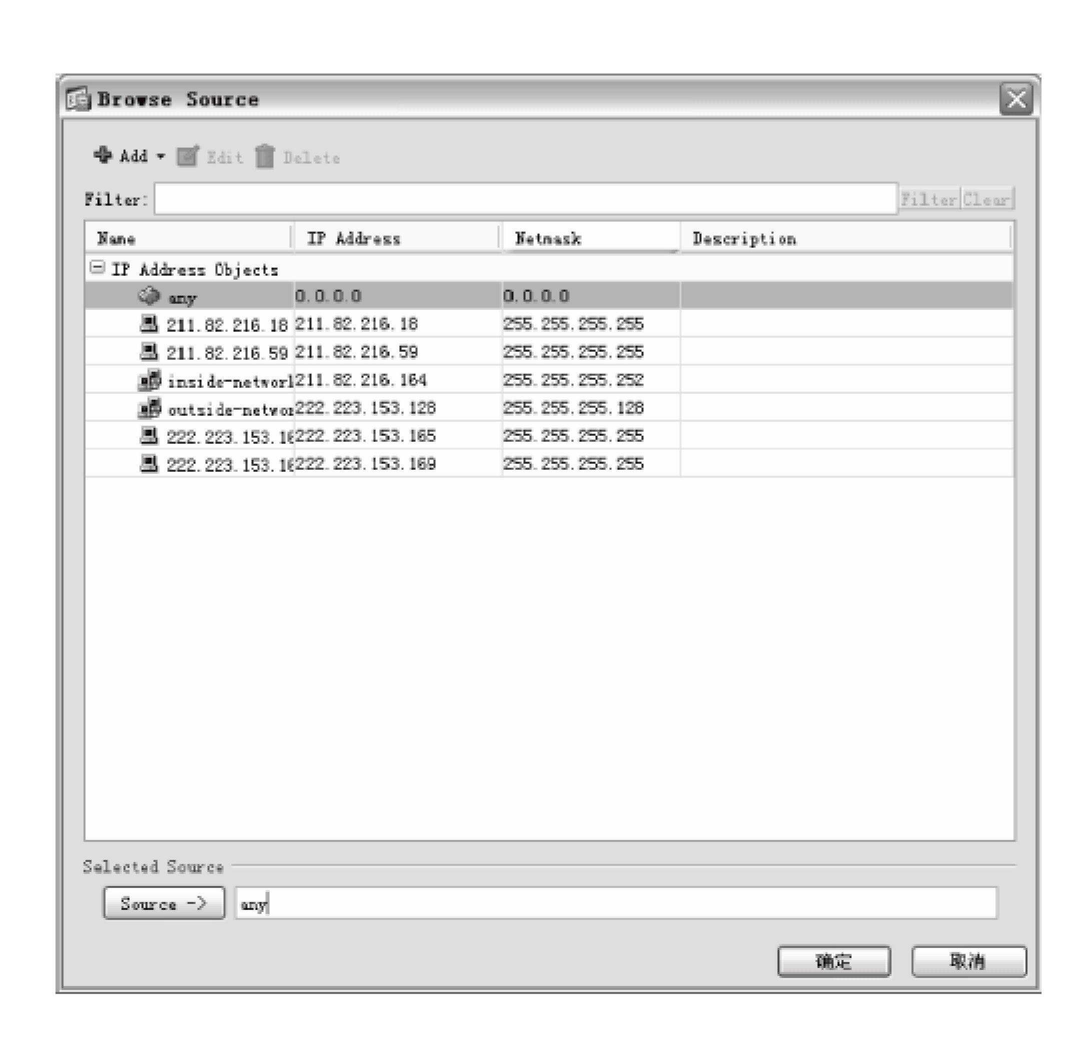


图 10-15　Browse Source 对话框

④ 在 Destination 下拉列表框中设置允许访问的目的 IP 地址，单击⊟按钮，显示图 10-16 所示的 Browse Destination 对话框。

⑤ 在 Service 下拉列表框中指定 IP 地址，单击⊟按钮，显示图 10-17 所示的 Browse Service 对话框。

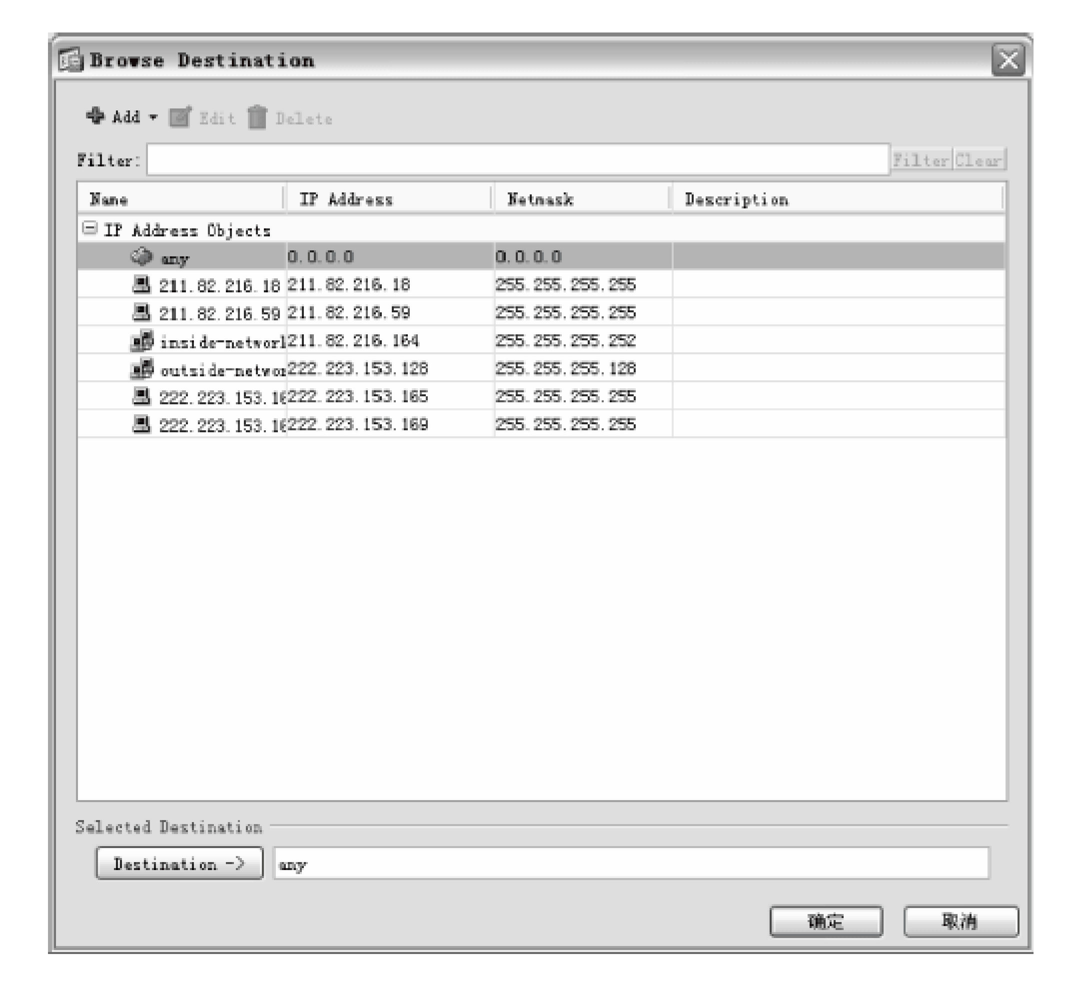


图 10-16　Browse Destination 对话框

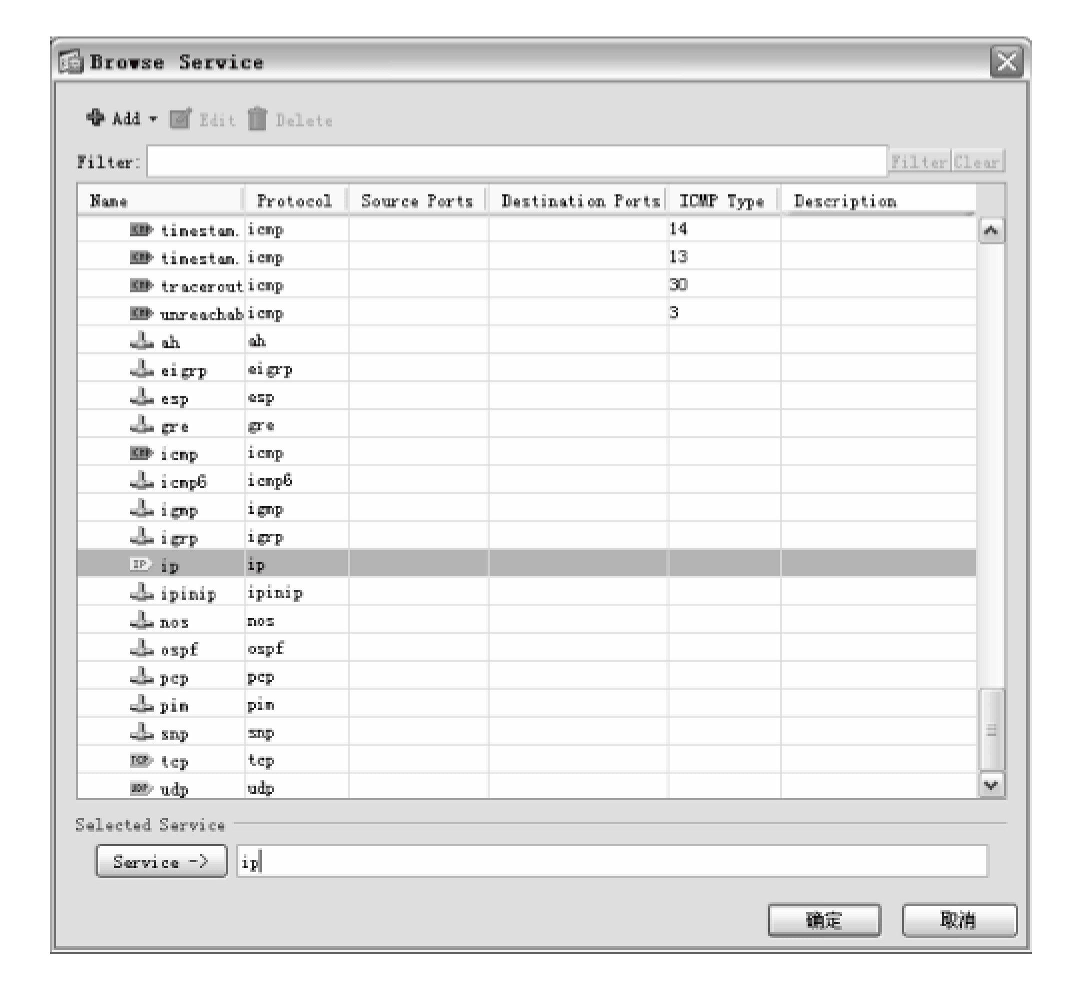


图 10-17　Browse Service 对话框

⑥ 在 Description 文本框中，输入 DMZ 描述信息。

⑦ 单击 More Options 下拉按钮，显示图 10-18 所示的 Add Access Rule 对话框。

⑧ 单击 Source Service 下拉列表框右侧的⊟按钮，显示图 10-19 所示的 Browse Source Service 对话框，添加 TCP 或 UDP 服务。具体内容参见相关内容，这里不再赘述。

⑨ 确认无误后，单击 OK 按钮，返回 Cisco ASDM 主页面，确认配置信息是否正确。然后，单击 Apply 按钮保存配置。此时，私有网络和 Internet 中的所有客户端，将都可以访问 DMZ 区中的 Web 服务了。

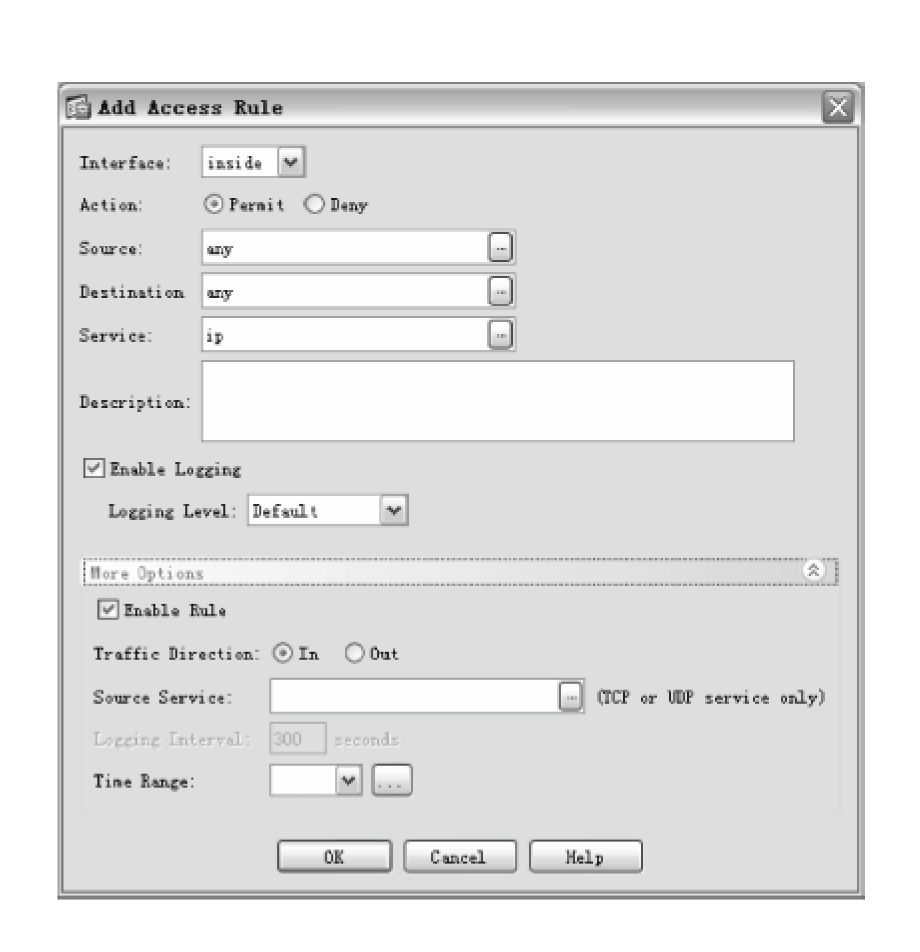




图 10-18 Add Access Rule 对话框

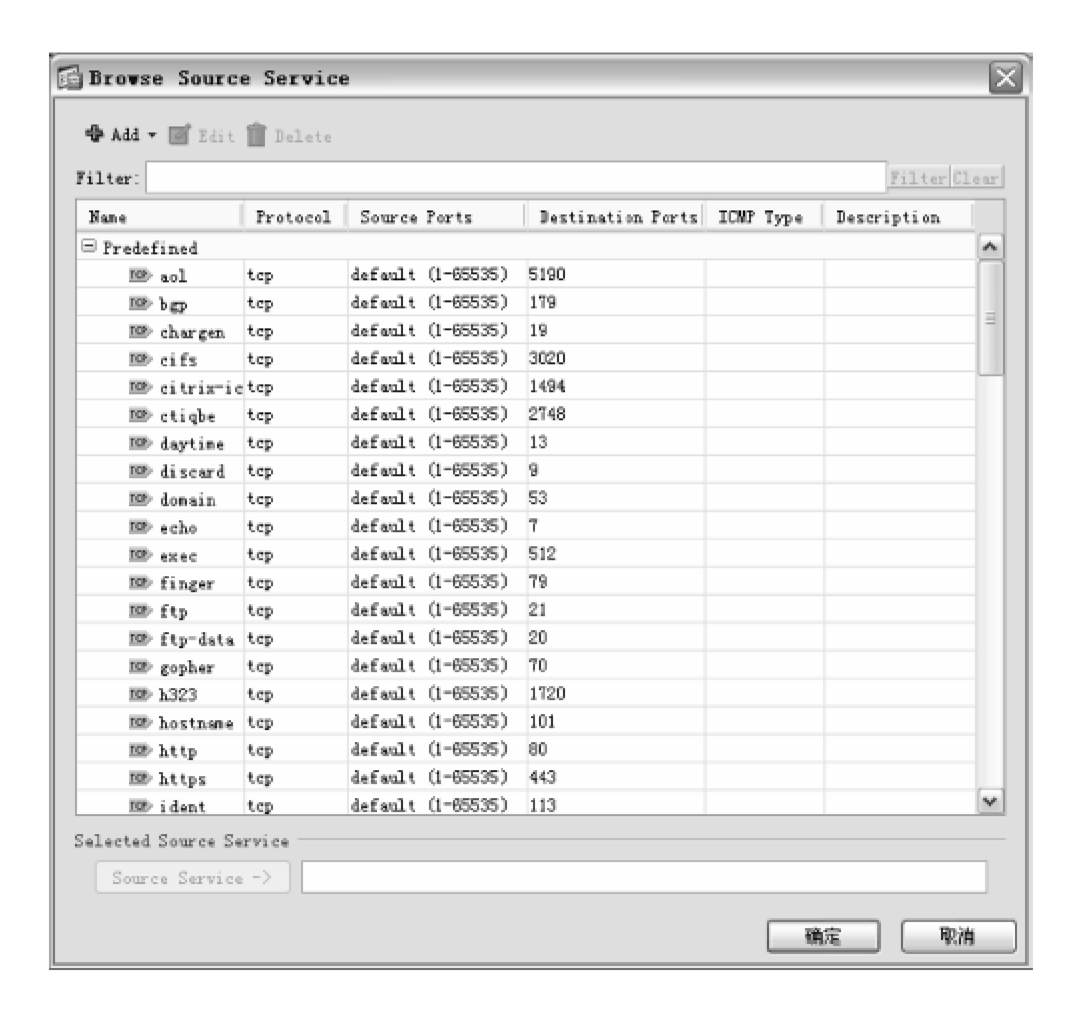


图 10-19 Browse Source Service 对话框

4. IPSec VPN 远程访问配置

IPSec VPN 远程访问非常适用于远程移动用户，借助 Internet 或其他公用网络，实现与公司网络的安全、廉价连接，图 10-20 所示为 IPSec VPN 远程访问的拓扑结构。

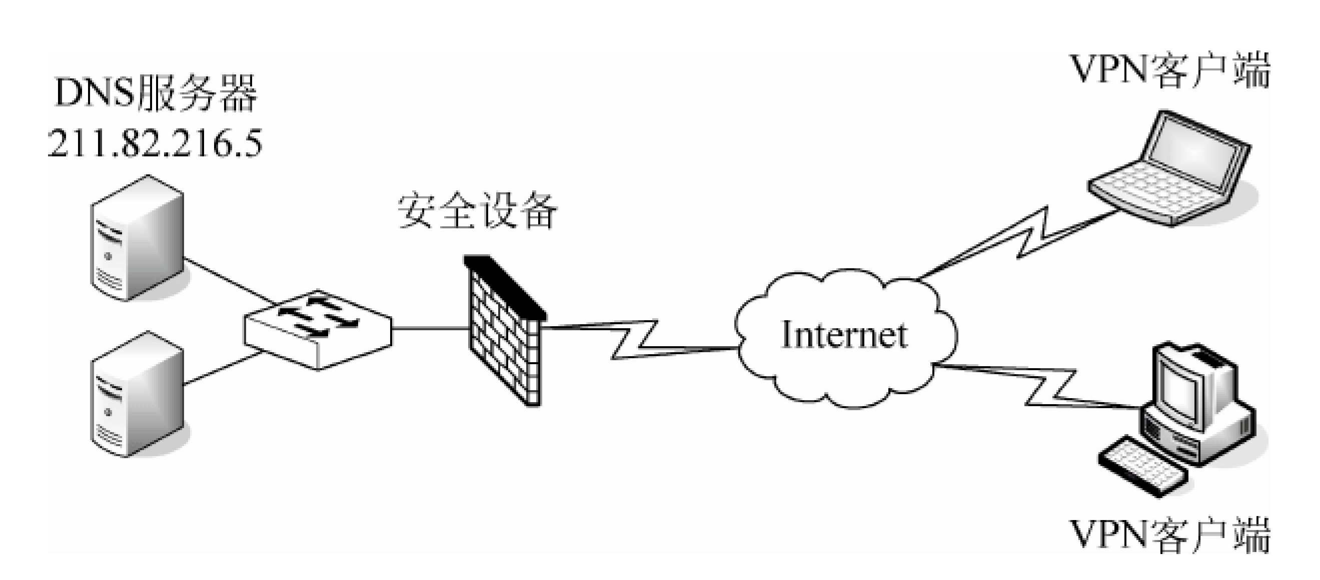


图 10-20 IPSec VPN 远程访问的拓扑结构

在配置 IPSec VPN 远程访问之前，需确认如下信息。

(1) IPSec VPN 远程客户端使用的 IP 地址池范围。

(2) 在本地认证数据库中创建用户列表，或者使用 AAA 服务器实现认证。

(3) 当 VPN 连接时，远程客户端使用的网络信息，包括：主 DNS 服务器和辅助 DNS 服务器的 IP 地址、默认域名和认证远程客户端可访问的本地主机、组和网络的 IP 地址列表。

配置 IPSec 远程访问 VPN 的步骤如下。

(1) 运行 Cisco ASDM 程序，显示图 10-21 所示的 A5510-SSLVPN 主窗口，在该窗口中显示设备的基本信息。

(2) 单击 Configuration 按钮，在左侧列表框中选择 Remote Access VPN 选项，配置远程访问 VPN，如图 10-22 所示。

配置远程访问 VPN 网络客户端访问包括以下内容。

① SSL VPN 连接配置文件。

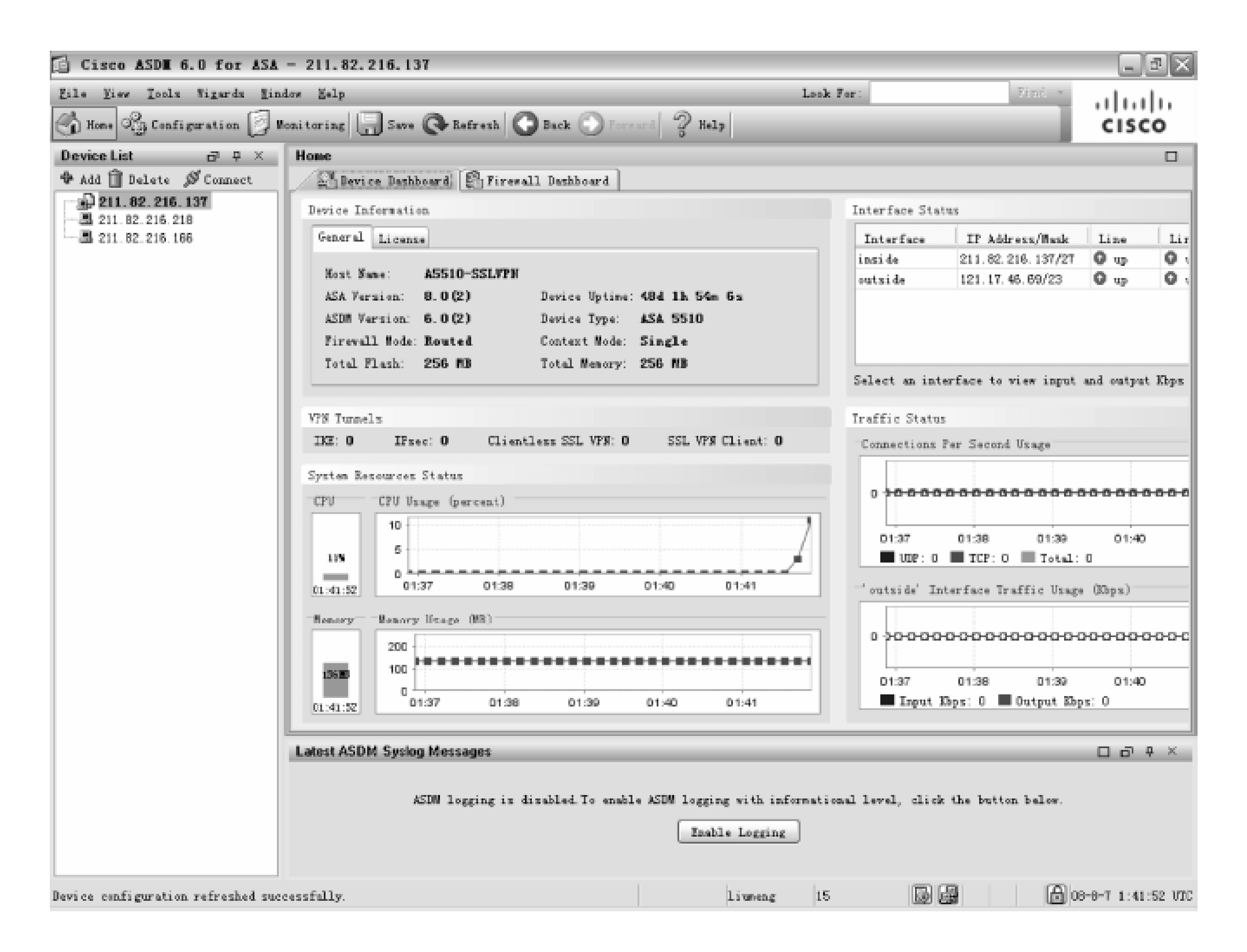


图 10-21　A5510-SSLVPN 主窗口

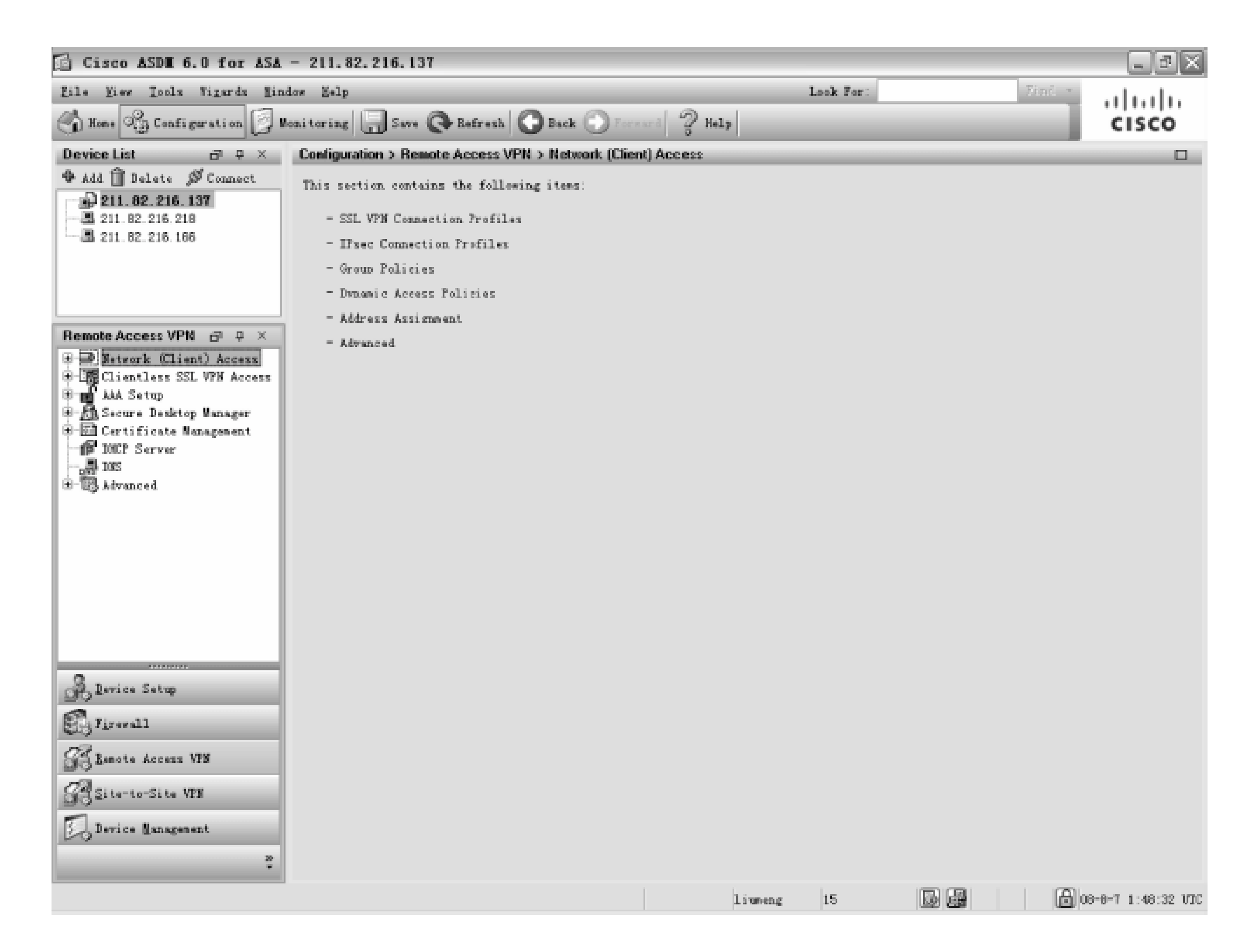


图 10-22　Remote Access VPN 选项

② IPSec 连接配置文件。

③ 组策略。

④ Dynamic 访问策略。

⑤ 地址分配。

⑥ 高级。

注意：VPN 向导包括 Startup Wizard 和 SSL VPN Wizard 两种。

(3) 依次选择 Wizards→Startup Wizard 命令，运行 VPN 向导，显示图 10-23 所示的 Startiing Point 对话框。根据需要选择起始点向导。

① 修改现有配置。

② 恢复出厂默认值配置。

(4) 选中 Modify existing configuration 单选按钮，单击 Next 按钮，显示图 10-24 所示的 Basic Configuration 对话框。分别在 ASA Host Name 和 Domain Name 文本框中，输入 ASA 主机名和域名。如果要启用特权模式密码，在 Privileged Mode (Enable) Password 选项区域中选中 Change privileged mode (enable) password 复选框，使用 ASDM 或命令行管理需启用特权模式的密码。

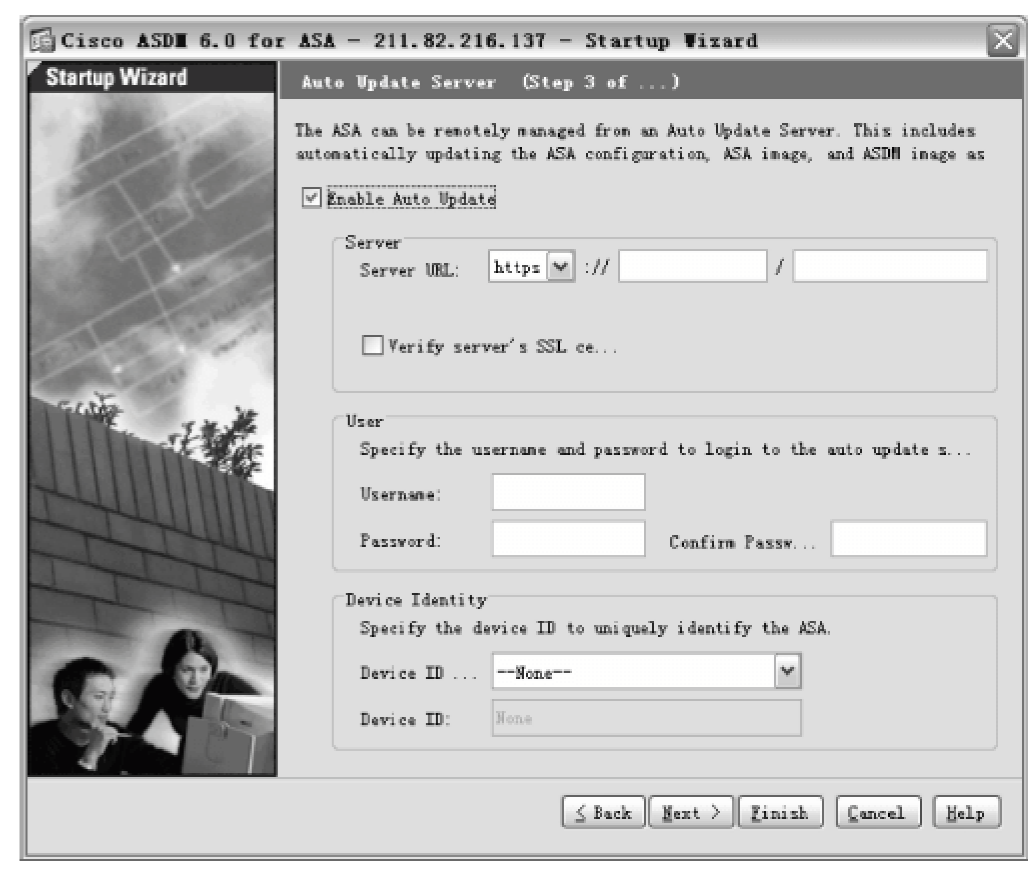


图 10-23 Startiing Point 对话框

图 10-24 Basic Configuration 对话框

(5) 单击 Next 按钮，显示图 10-25 所示的 Auto Update Server 对话框，如果要启用自动更新服务器远程管理，选中 Enable Auto Update 复选框，分别在 Server、User 和 Device Identity 选项区域中，输入 Server URL、Username、Password 和 Device ID 信息。

(6) 单击 Next 按钮，显示图 10-26 所示的 Outside Interface Configuration 对话框，配置与 ISP 提供商进行连接的接口。



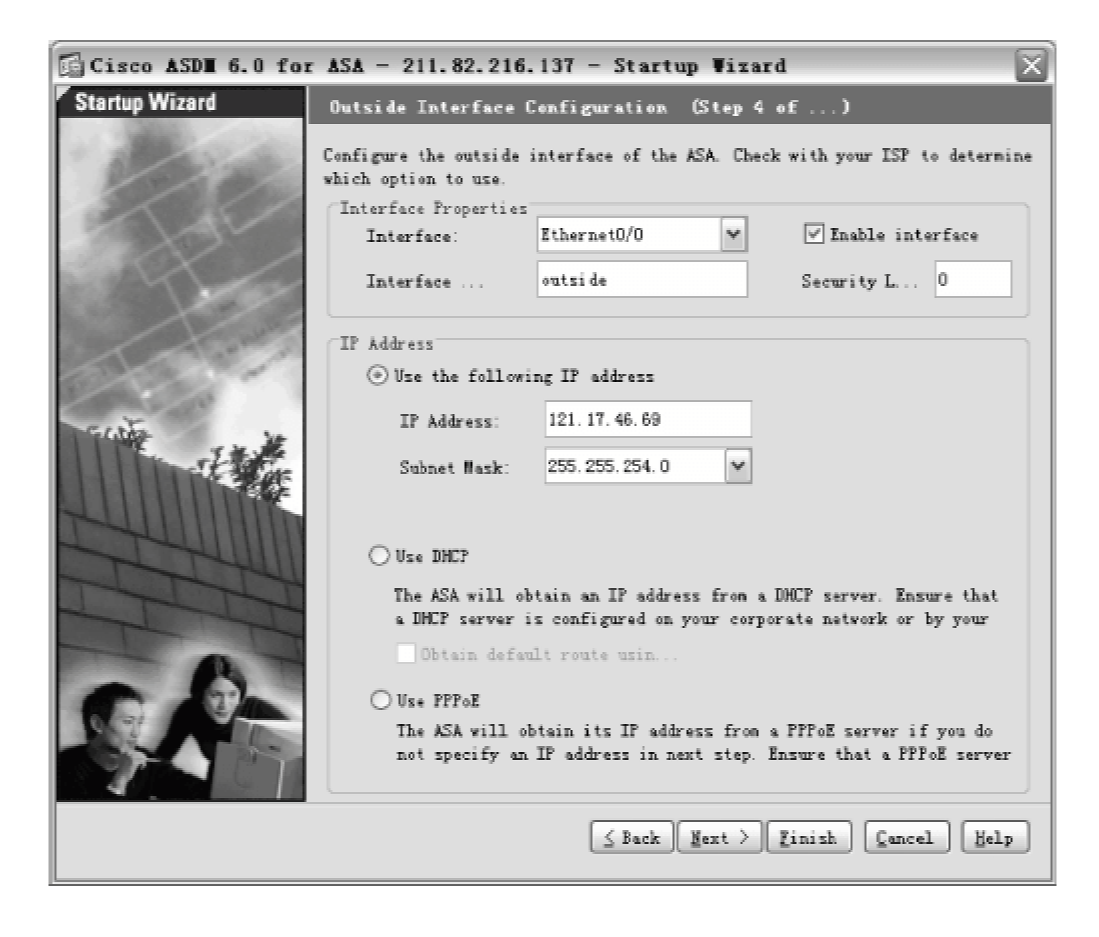




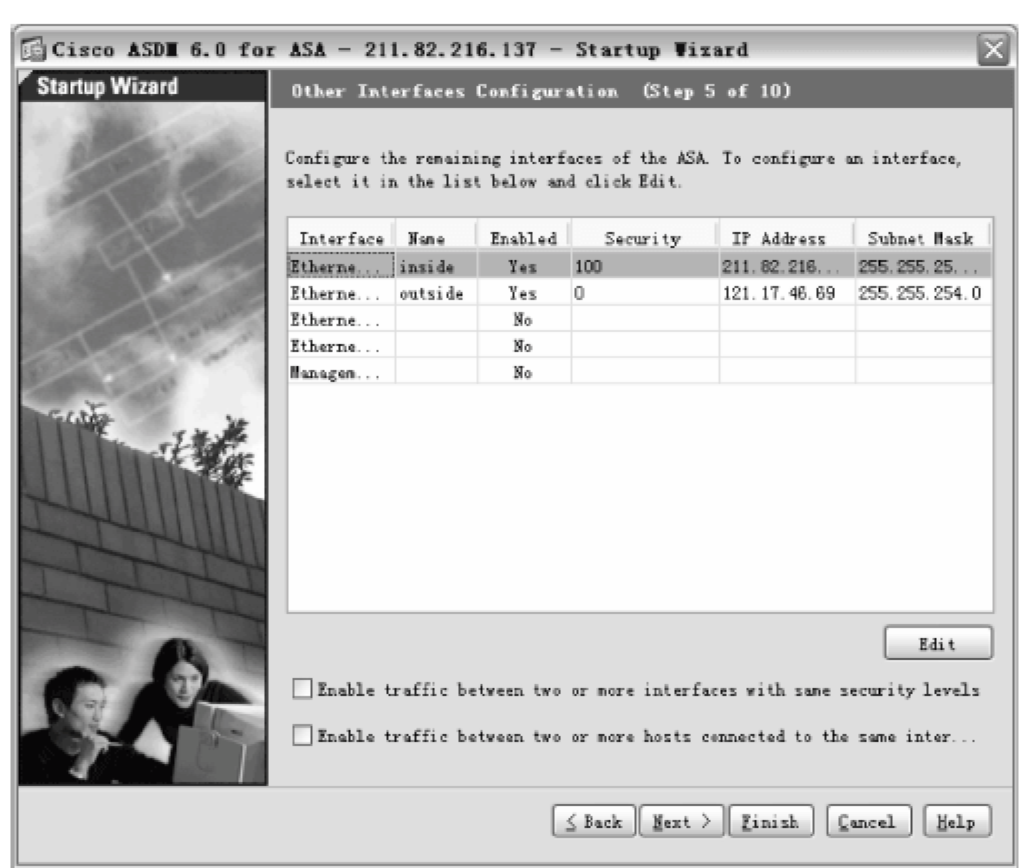
图 10-25 Auto Update Server 对话框

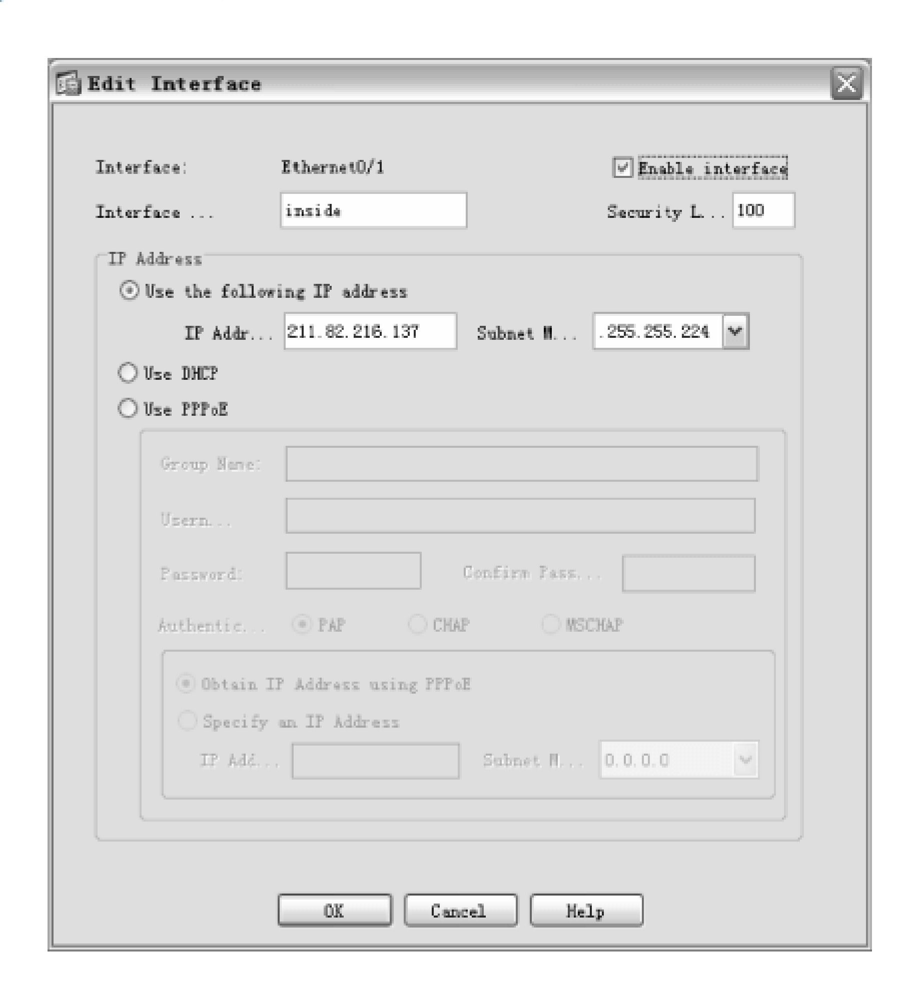
图 10-26 Outside Interface Configuration 对话框

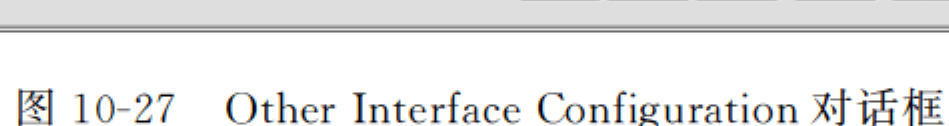
(7) 单击 Next 按钮，显示图 10-27 所示的 Other Interface Configuration 对话框。

(8) 单击 Edit 按钮，显示图 10-28 所示的 Edit Interface 对话框，编辑端口信息。编辑

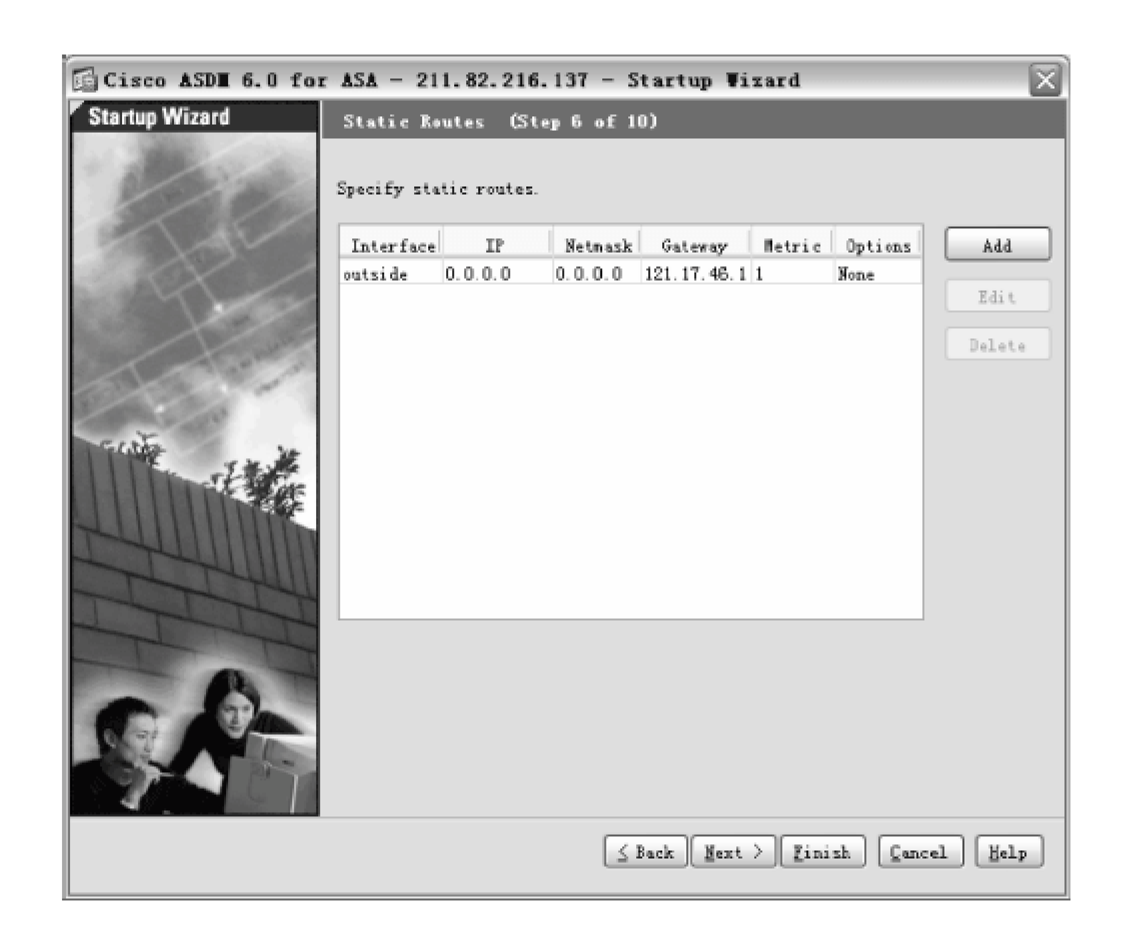
完后单击 OK 按钮，返回到 Other Interface Configuration 对话框。






图 10-27　Other Interface Configuration 对话框　　图 10-28　Edit Interface 对话框

(9) 单击 Next 按钮，显示图 10-29 所示的 Static Routes 对话框，指定静态路由。单击 Add 按钮，显示图 10-30 所示的 Add Static Route 对话框，添加静态路由。



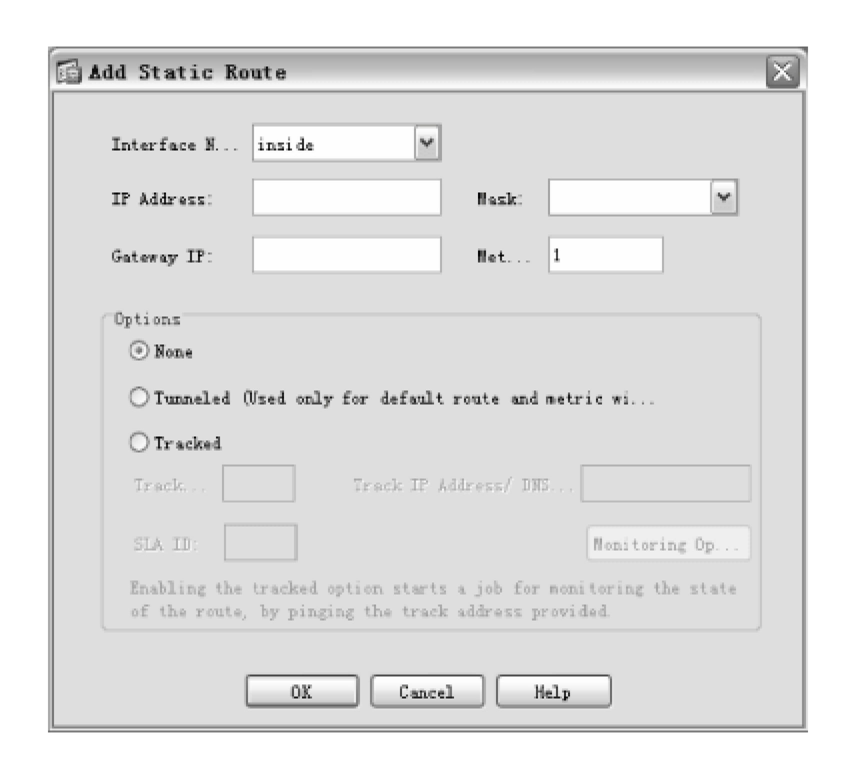


图 10-29　Static Routes 对话框　　图 10-30　Add Static Route 对话框

单击 Edit 按钮，显示图 10-31 所示的 Edit Static Route 对话框，编辑静态路由。

(10) 单击 Next 按钮，显示图 10-32 所示 DHCP Server 对话框。可以启动 ASA DHCP 服务器功能，根据需要启用 DHCP 服务器的内部端口，设置 DHCP 服务器的参数即可。

(11) 单击 Next 按钮，显示图 10-33 所示的 Address Translation 对话框，根据需要设置地址转换(NAT/PAT)即可。

(12) 单击 Next 按钮，显示图 10-34 所示的 Administrative Access 对话框，指定所有主机或允许访问使用 HTTPS/ASDM、SSH 或 Telnet 的网络地址。

单击 Add 按钮，显示图 10-35 所示的 Add Administrative Access Entry 对话框。添加管理访问项，单击 OK 按钮返回即可。

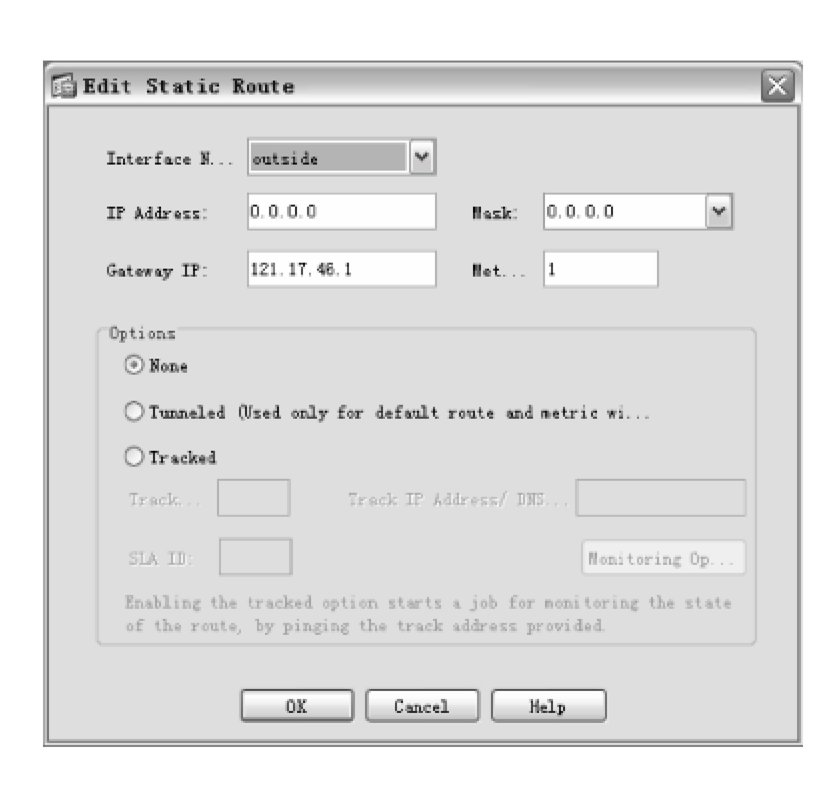


图 10-31　Edit Static Route 对话框

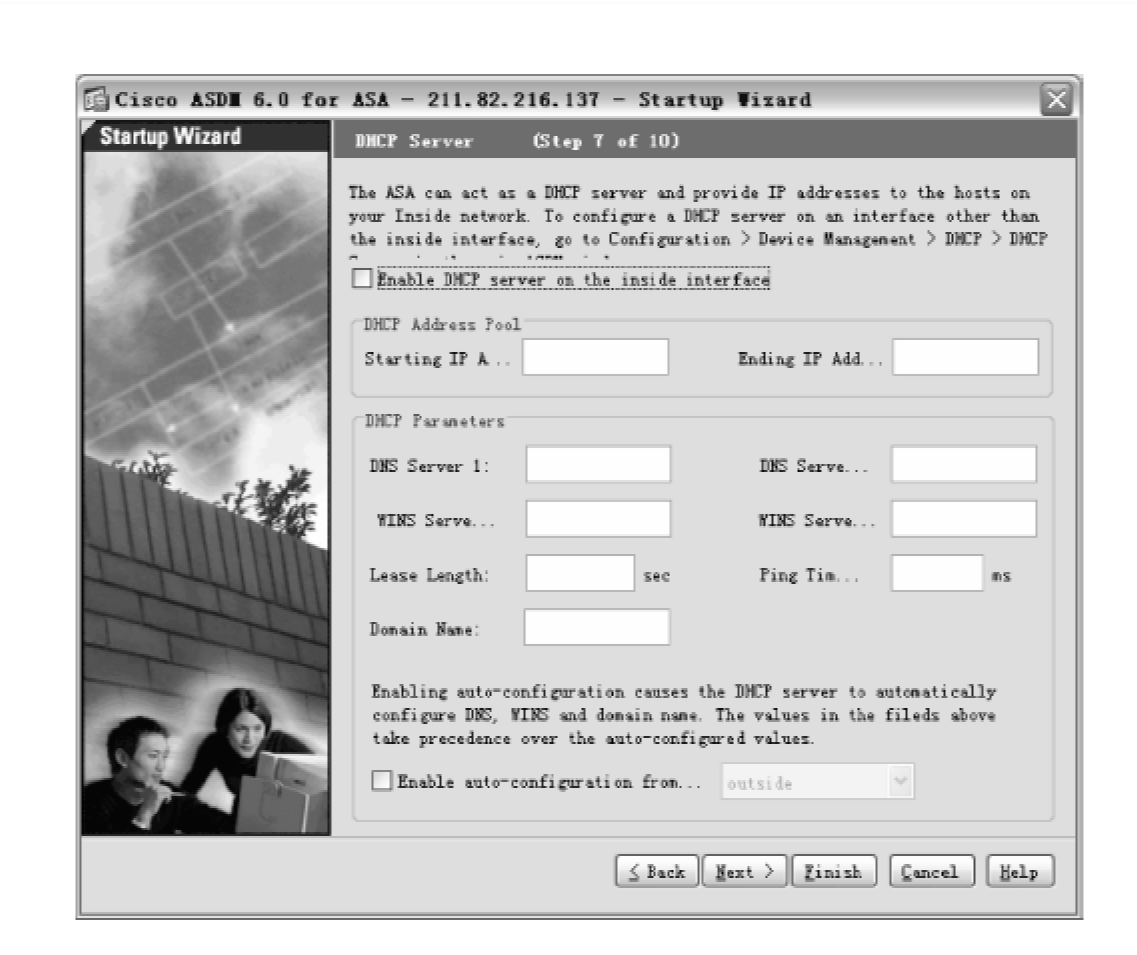


图 10-32　DHCP Server 对话框



图 10-33　Address Translation 对话框

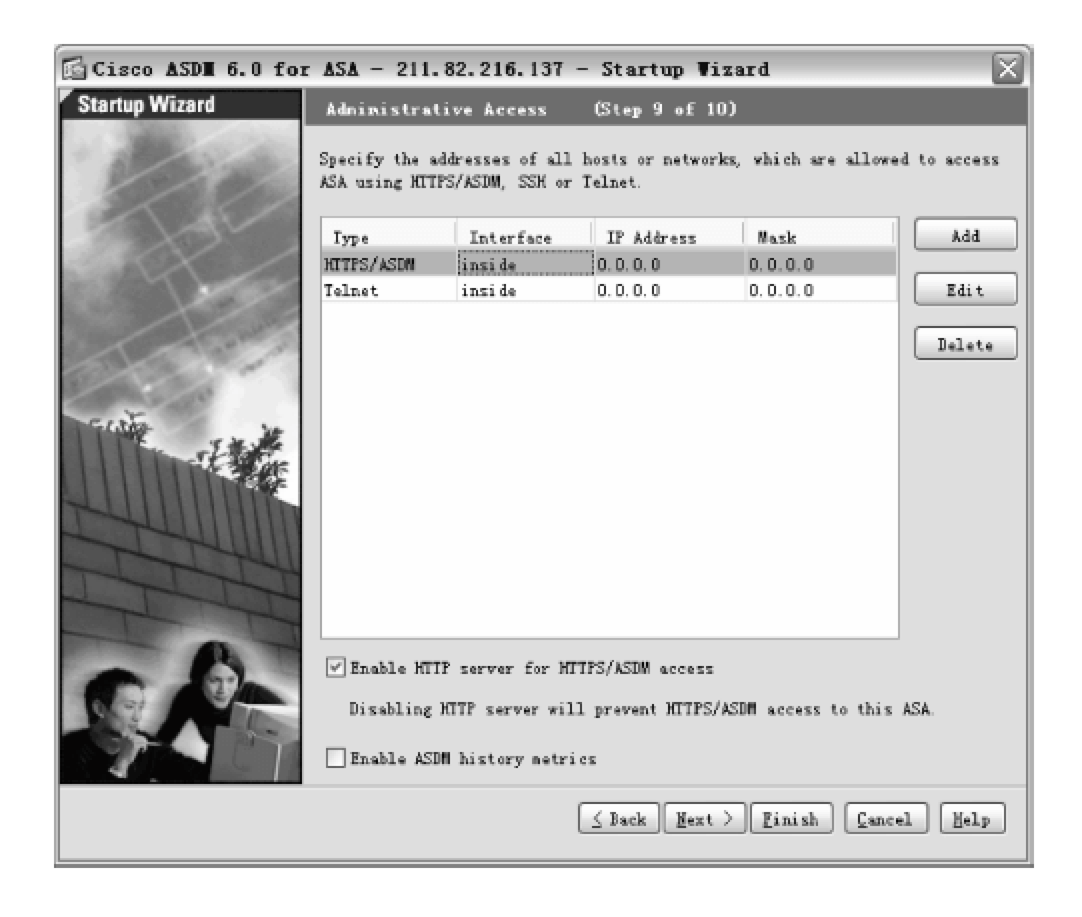


图 10-34　Administrative Access 对话框

（13）单击 Next 按钮，显示图 10-36 所示的 Startup Wizard Summary 对话框，显示启动向导摘要，检查是否正确。

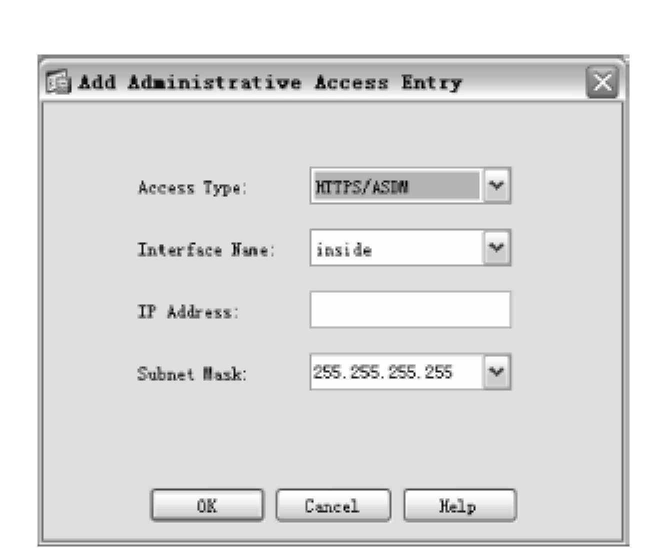


图 10-35　Add Administrative Access Entry 对话框

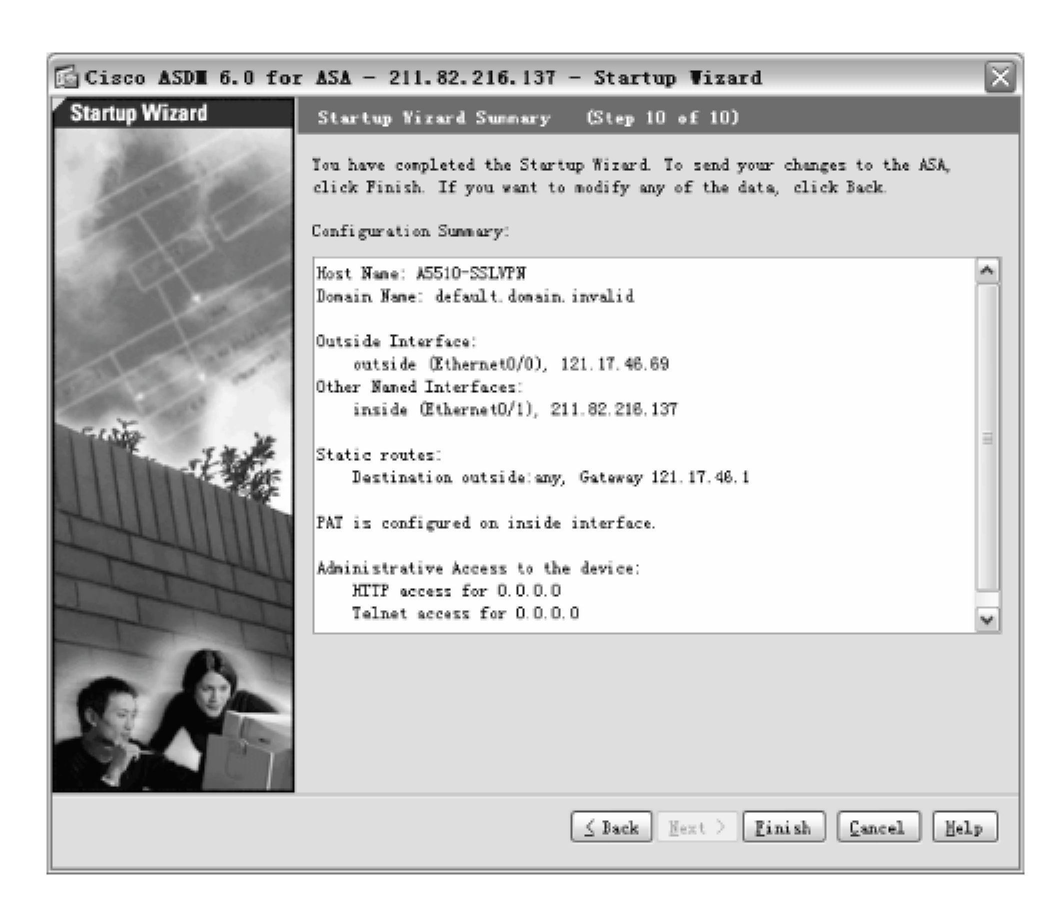


图 10-36　Startup Wizard Summary 对话框

（14）单击 Finish 按钮，完成 VPN 配置并保存。

使用 SSL VPN 向导，配置 IPsec VPN 远程访问。

（1）依次选择 Wizards→SSL VPN Wizard 命令，运行 VPN 向导，显示图 10-37 所示的 SSL VPN Connection Type 对话框。

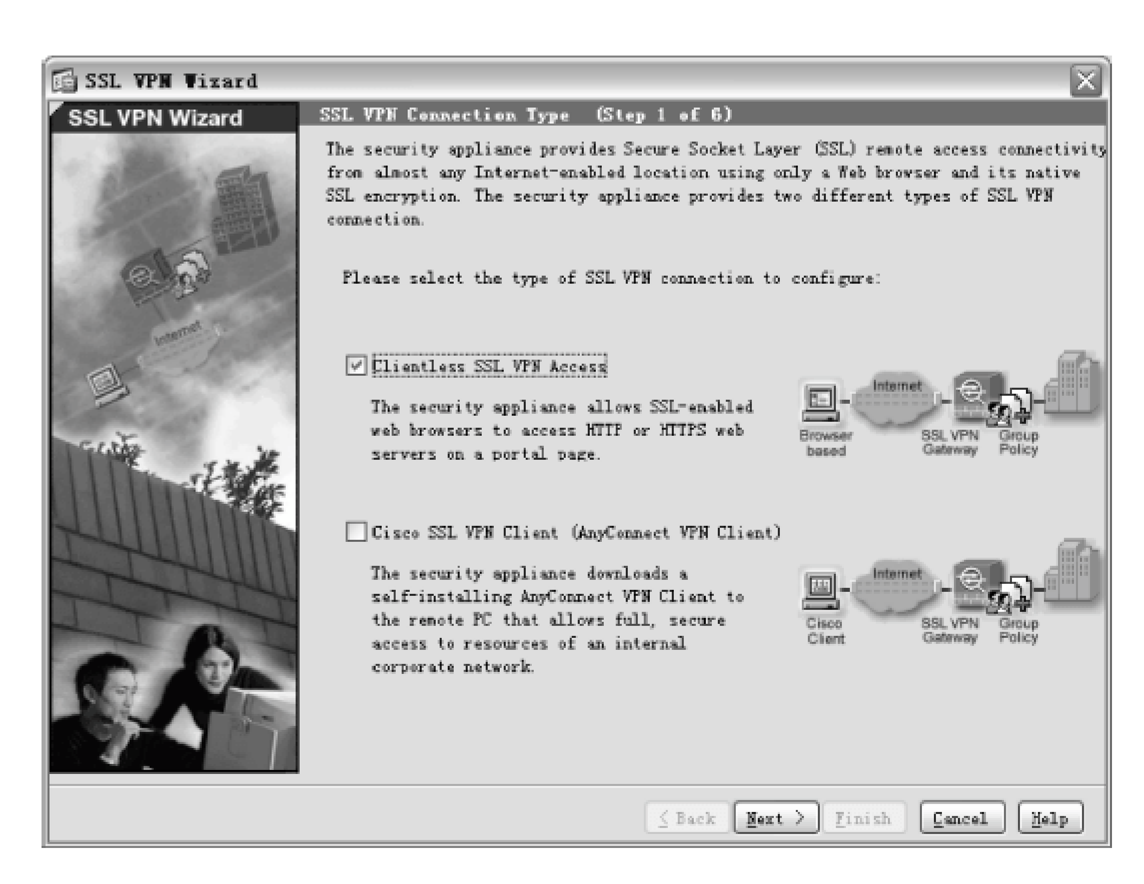


图 10-37 SSL VPN Connection Type 对话框

（2）单击 Next 按钮，显示图 10-38 所示的 SSL VPN Interface 对话框。

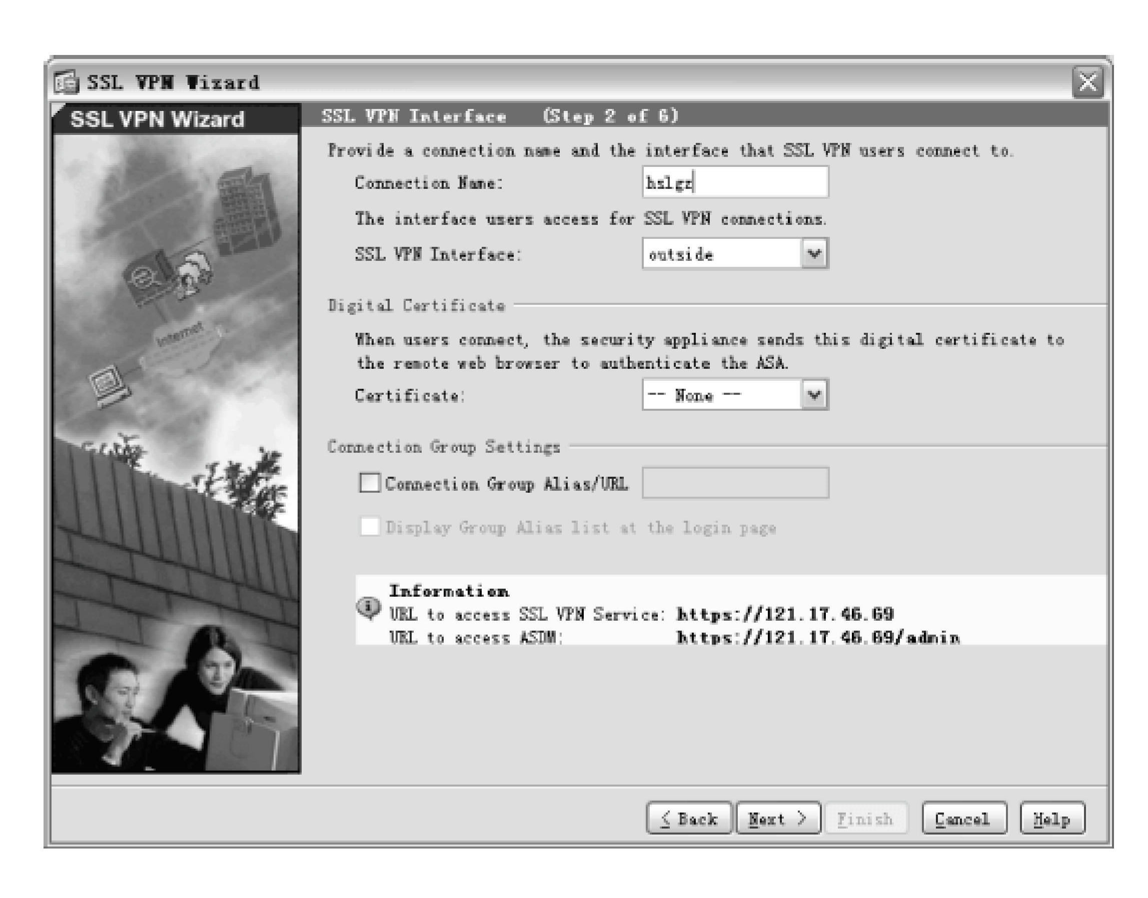


图 10-38 SSL VPN Interface 对话框

（3）单击 Next 按钮，显示图 10-39 所示的 User Authentication 对话框，设置用户身份验证。如果选择本地用户数据库验证用户，既可以在这里创建新用户账号，也可以稍后使用 ASDM 配置界面添加用户。在 Username、Password 和 Confirm Password 中分别输入用户名、密码、确认密码，单击 Add 按钮，即可向本地用户数据库中添加新的用户。重复操作，可添加多个用户。

（4）单击 Next 按钮，显示图 10-40 所示的 Group Policy 对话框，可以创建新的组策略。

（5）单击 Next 按钮，显示图 10-41 所示的 Clientless Connections Only - Bookmark List 对话框，根据需要设置连接客户端的书签列表。

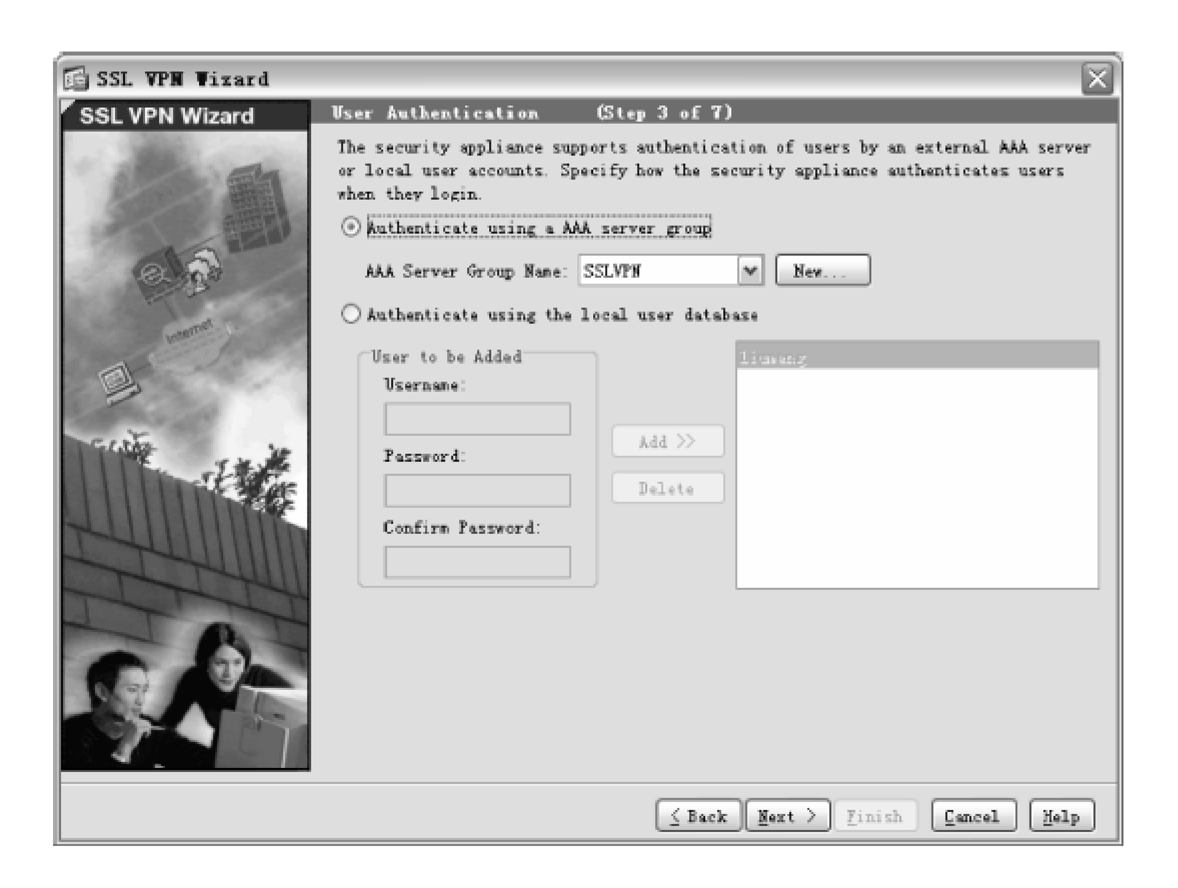


图 10-39　User Authentication 对话框



图 10-40　Group Policy 对话框

（6）单击 Manage 按钮，显示图 10-42 所示的 Configure GUI Customization Objects 对话框，配置 SSL VPN 门户网站页面显示的安全设备的书签列表。



图 10-41　Clientless Connections Only - Bookmark List 对话框

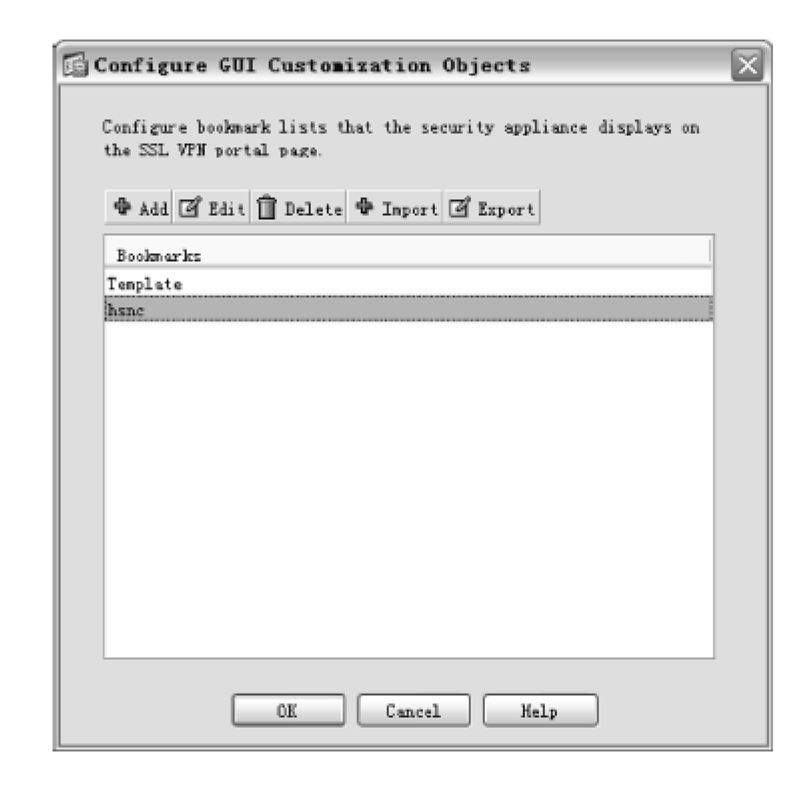


图 10-42　Configure GUI Customization Objects 对话框

(7) 单击 Edit 按钮，显示图 10-43 所示的 Edit Bookmark List 对话框。根据需要，可以添加、编辑、删除书签。

(8) 单击 Add 按钮，显示图 10-44 所示的 Add Bookmark Entry 对话框，添加书签项。

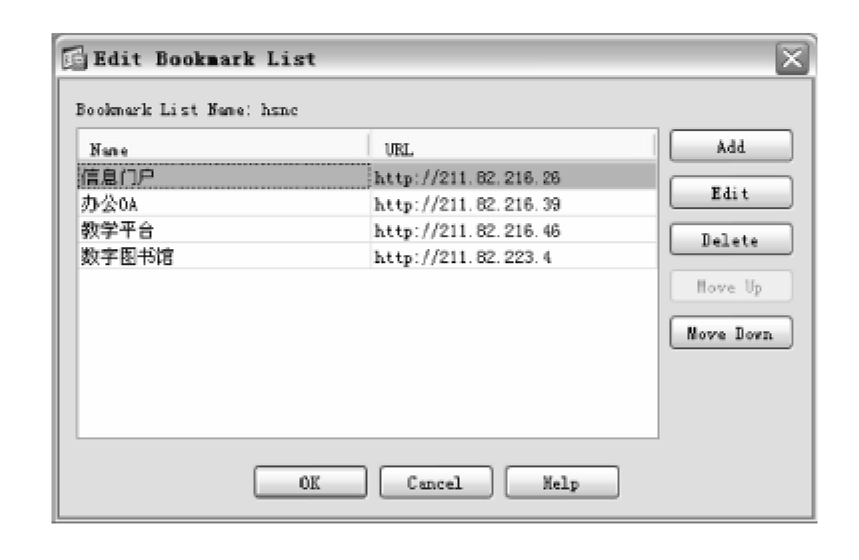


图 10-43 Edit Bookmark List 对话框



图 10-44 Add Bookmark Entry 对话框

(9) 连续单击 OK 按钮，显示图 10-45 所示的 Clientless Connections Only - Bookmark List 对话框，连接书签列表。



图 10-45 Clientless Connections Only - Bookmark List 对话框

(10) 单击 Next 按钮，显示图 10-46 所示的 Summary 对话框，显示已创建 SSL VPN 摘要信息。



图 10-46 Summary 对话框

(11) 单击 Finish 按钮，完成 SSL VPN 配置并保存。

5. Site-to-Site VPN 配置

借助 Site-to-Site VPN 配置，可以实现远程网络的廉价安全互联，特别适用于总公司与分部之间的相互连接，图 10-47 所示为网络层的 Site-to-Site VPN 拓扑结构。

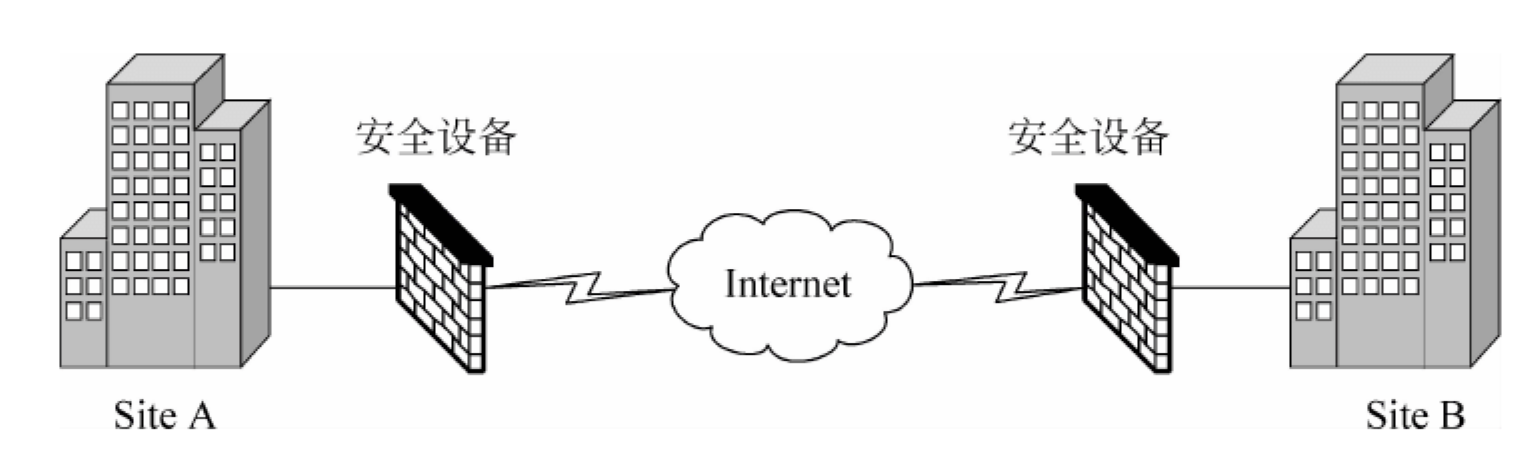


图 10-47 网络层的 Site-to-Site VPN 拓扑结构

在开始配置之前，应确认已经准备好以下数据。

(1) 对端远程安全设备的 IP 地址。

(2) 允许使用隧道连接与远程站点上的资源通信的本地主机和网络的 IP 地址。

(3) 允许使用隧道与本地资源通信的远程主机和网络的 IP 地址。

配置 Site-to-Site VPN 的步骤如下。

(1) 在 A5510-SSLVPN 主窗口中，单击 Configuration 按钮，在左侧列表框中选择 Site-to-Site VPN 选项，配置远程访问 VPN，显示图 10-48 所示的 Site-to-Site VPN 对话框。

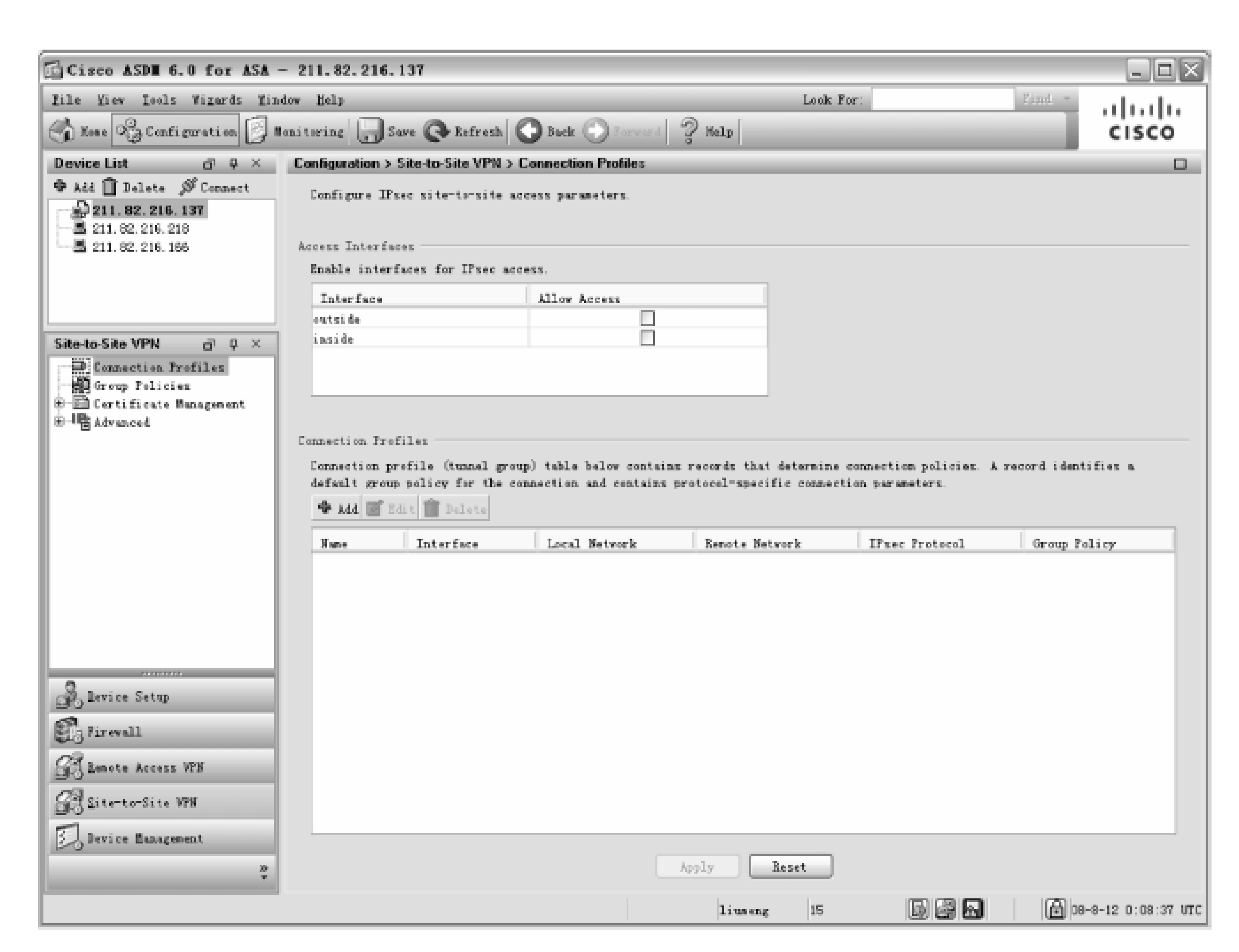


图 10-48 Site-to-Site VPN 对话框

(2) 依次选择 Wizard→IPSec VPN Wizard 命令，运行 VPN 向导，显示图 10-49 所示的 VPN Tunnel Type 对话框。配置本地站点安全设备，选中 Site-to-Site 单选按钮，从 VPN Tunnel Interface 下拉列表框中选择 outside 选项。

(3) 单击 Next 按钮，显示图 10-50 所示的 Remote Site Peer 对话框，在 Peer IP Address 文本框中，输入对端安全设备的 IP 地址(如 121.17.46.68)，在 Tunnel Group Name 文本框中，输入隧道组名称，并在 Authentication Method 选项区域选择认证方式。

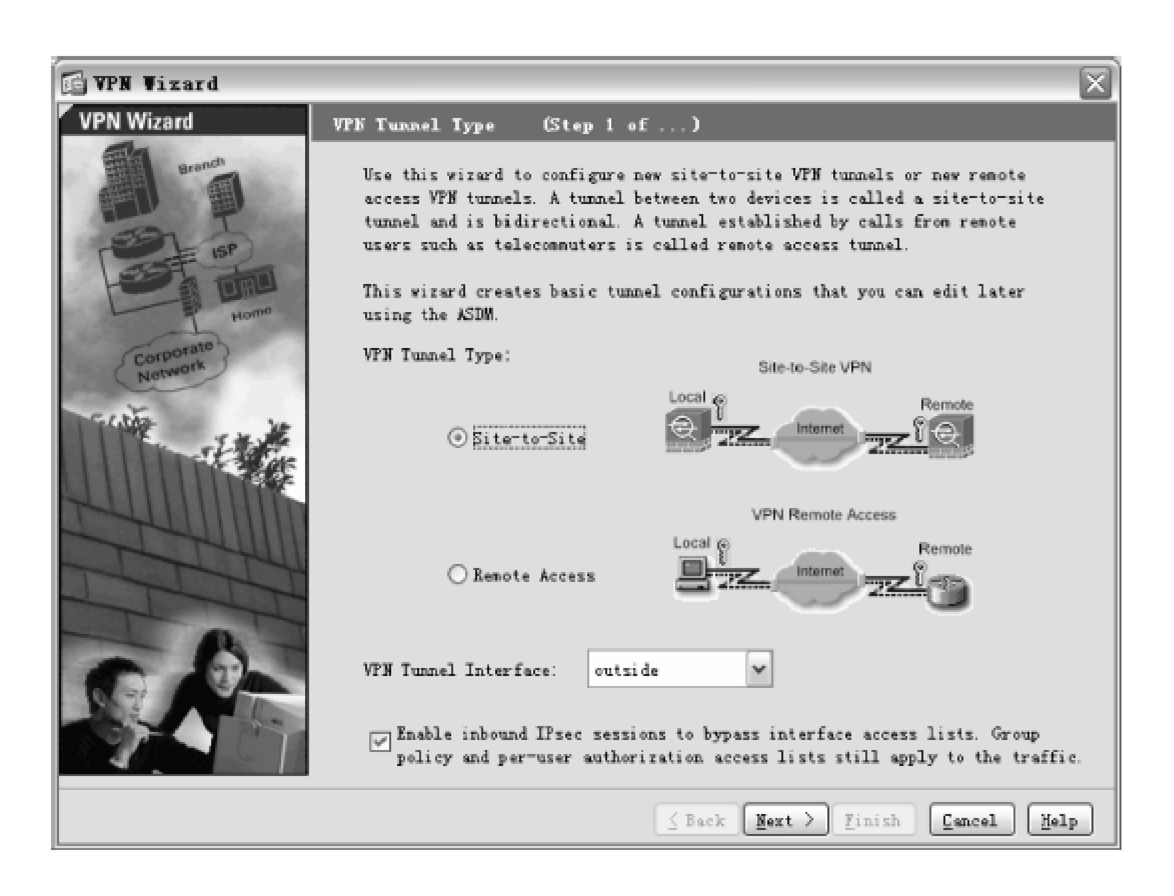


图 10-49　VPN Tunnel Type 对话框



图 10-50　Remote Site Peer 对话框

具体认证方式的选择，参见上述相关内容。

（4）单击 Next 按钮，显示图 10-51 所示的 IKE Policy 对话框，配置 IKE 策略。采用 ASDM 的系统默认值，即可在两个安全设备之间创建安全的 VPN 隧道。



图 10-51　IKE Policy 对话框

(5) 单击 Next 按钮,显示图 10-52 所示的 IPsec Encryption and Authentication 对话框,配置 IPsec 加密和认证参数。详细设置参见上述相关内容,这里不再赘述。



图 10-52 IPsec Encryption and Authentication 对话框

(6) 单击 Next 按钮,显示图 10-53 所示的 Host and Networks 对话框,指定主机和网络。在 Local Networks 文本框中,选择 IP 地址对象,如图 10-54 所示。单击确定按钮返回即可。



图 10-53 Host and Networks 对话框

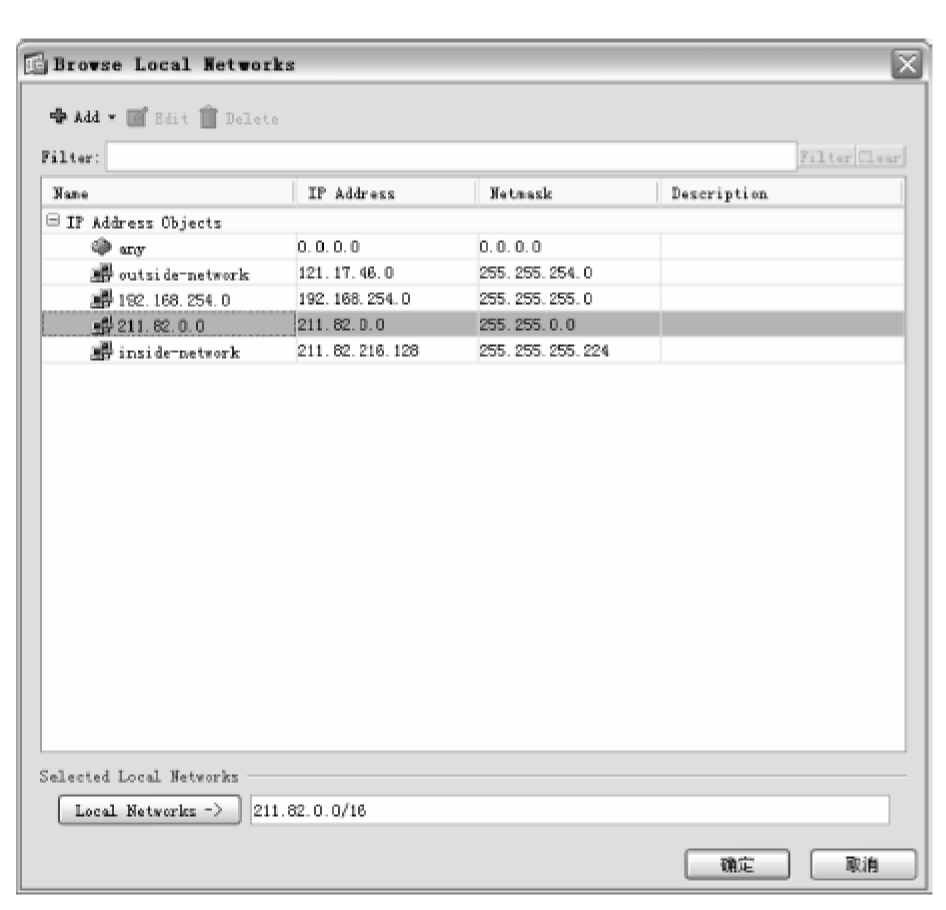


图 10-54 Browse Local Networks 对话框

(7) 单击 Next 按钮,显示图 10-55 所示的 Summary 对话框,显示 VPN 配置的汇总信息。

(8) 检查无误后,单击 Finish 按钮,返回 ASDM 主窗口。若欲将修改后的配置保存至启用配置(Startup Configuration),当设备下一次启动时应用,还应在 File 菜单中选择 Save 命令。

(9) 配置对端另一台 VPN 设备,应确保两端的相关参数保持一致。

6. 管理安全设备

使用 Cisco 自适应安全设备管理器管理安全设备,可以通过 Web 图形界面监视设备的运行状态、查看和分析网络流量、查看和分析系统日志和安全监控工具,使管理员能够更好



图 10-55 Summary 对话框

地管理安全设备。

(1) 监视安全设备运行状态

利用 Cisco ASDM 登录到 Cisco ASA 主界面，如图 10-56 所示，在主页中可以看到 Device Dashboard 选项卡中显示设备信息(名称、版本、型号等)、系统资源运行状态(CPU 和 Memory)、接口状态和信息传输状态。

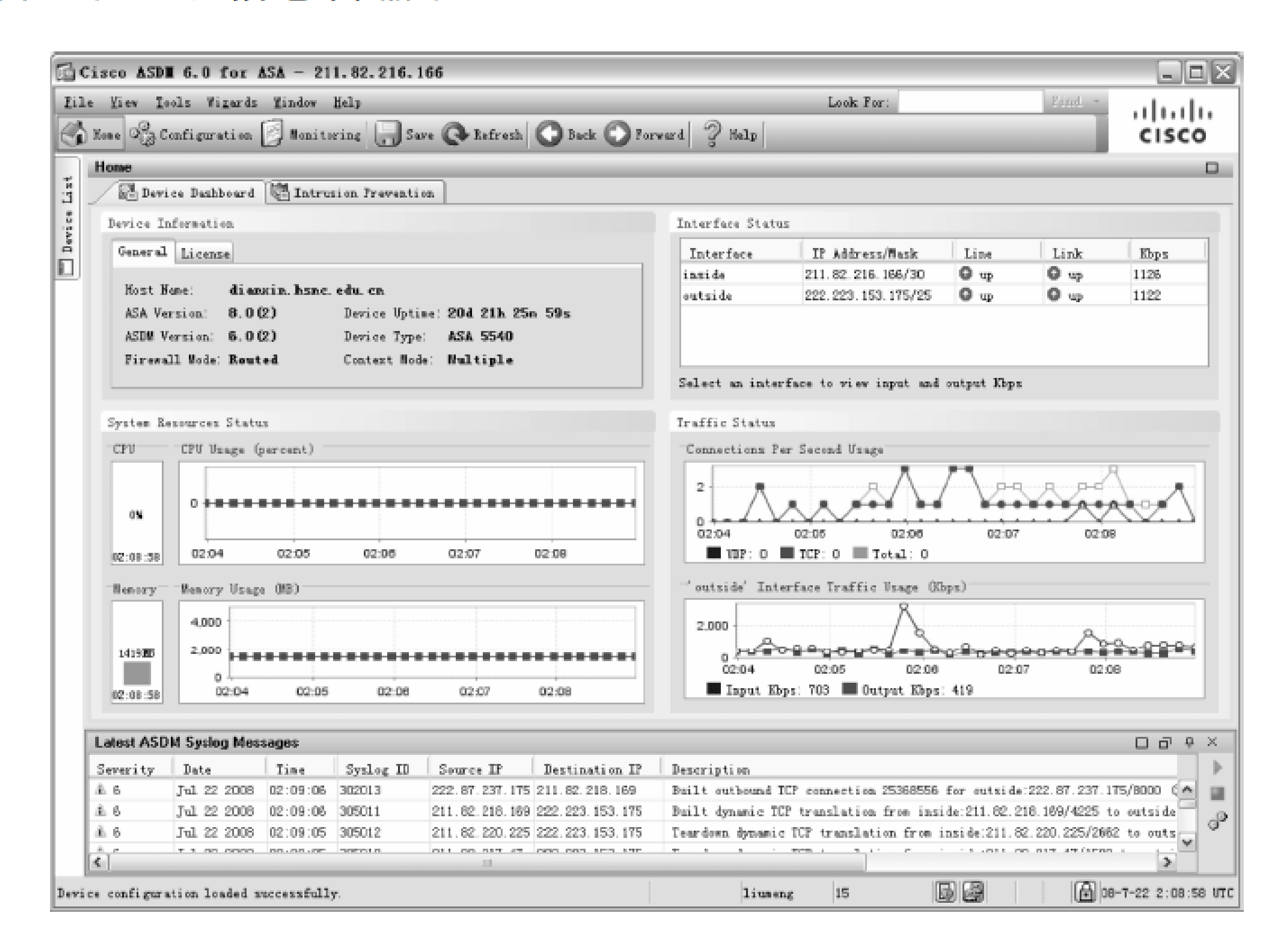


图 10-56 Cisco ASA 主界面

(2) 查看和分析网络流量

通常情况下，网络安全设备位于网络的主干处，所以安全设备的流量即为网络的所有流量。通过对这些流量进行查看和分析，即可发现网络中的非法流量，并根据分析结果进行排除即可。

① 在 Cisco ASA 主界面中，单击 Monitoring 按钮，监视设备的接口信息，如图 10-57 所示。

② 在左侧 Interfaces 列表栏中选择 Interface Graphs 选项，可以查看内部或外部的接口

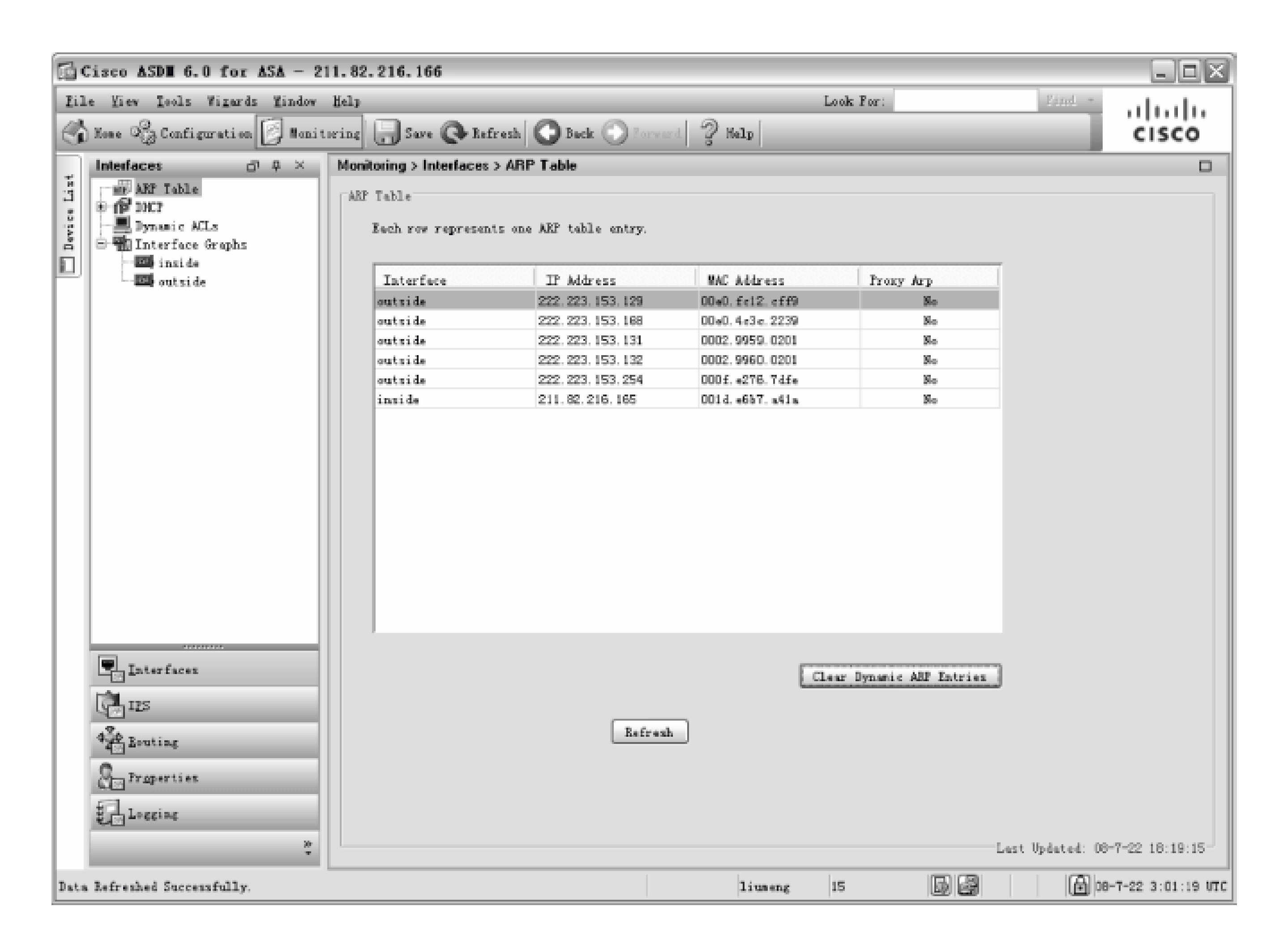


图 10-57 监视设备的接口信息

图表，如图 10-58 所示。

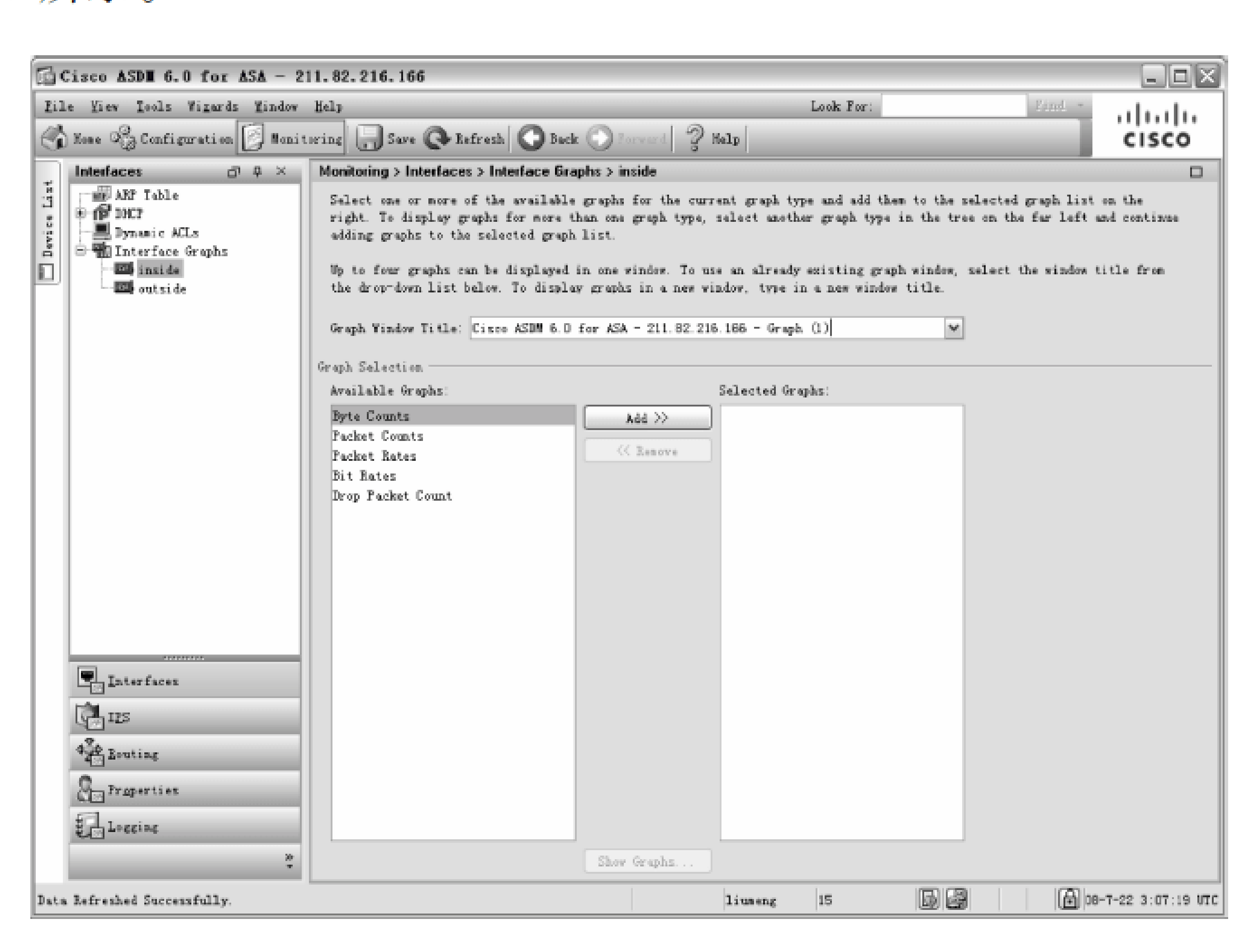


图 10-58 Interface Graphs 窗口

③ 以内部接口为例，在 Graph Selection 选项区域中显示图形所选内容，在 Available Graphs 列表框中，选择可用图形并添加到 Selected Graphs 列表框中，如图 10-59 所示。

④ 单击 Show Graphs 按钮，以图例形式显示网络的流量，如图 10-60 所示。

(3) 查看和分析系统日志

与交换机和路由器等设备相同，网络安全设备同样有其日志文件。通过查看和分析系统日志文件，可以更进一步地了解安全设备的工作状态，以及发生故障时的日志信息等。

① 在 Cisco ASA 主页左侧栏中，选择 Logging 选项，显示图 10-61 所示的 Real-Time Log Viewer 对话框，在 Logging Level 下拉列表中选择日志记录级别。在 Buffer Limit 文本框中输入缓冲区限制，一般为默认值即可。

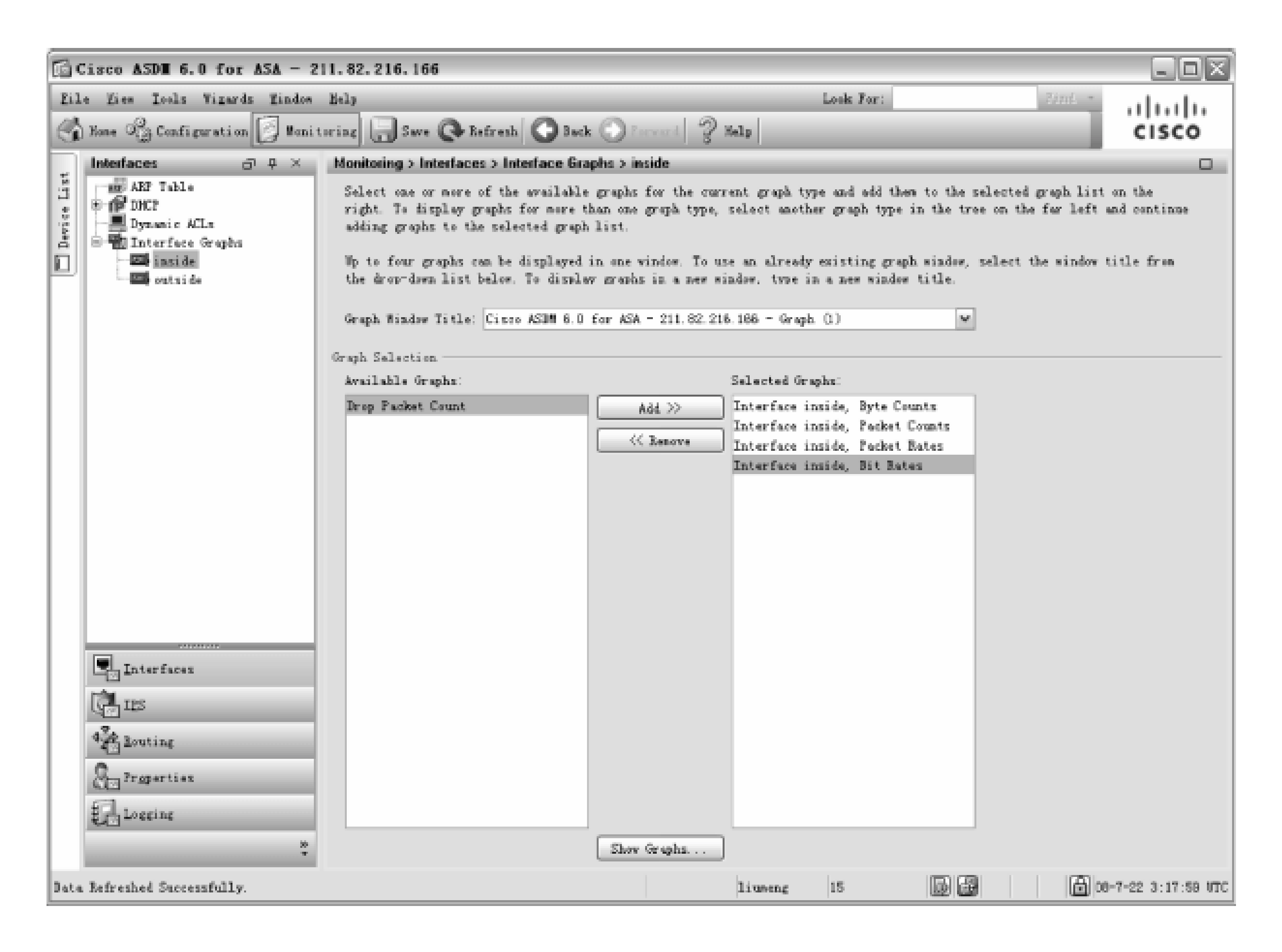


图 10-59　Graph Selection 选项区域

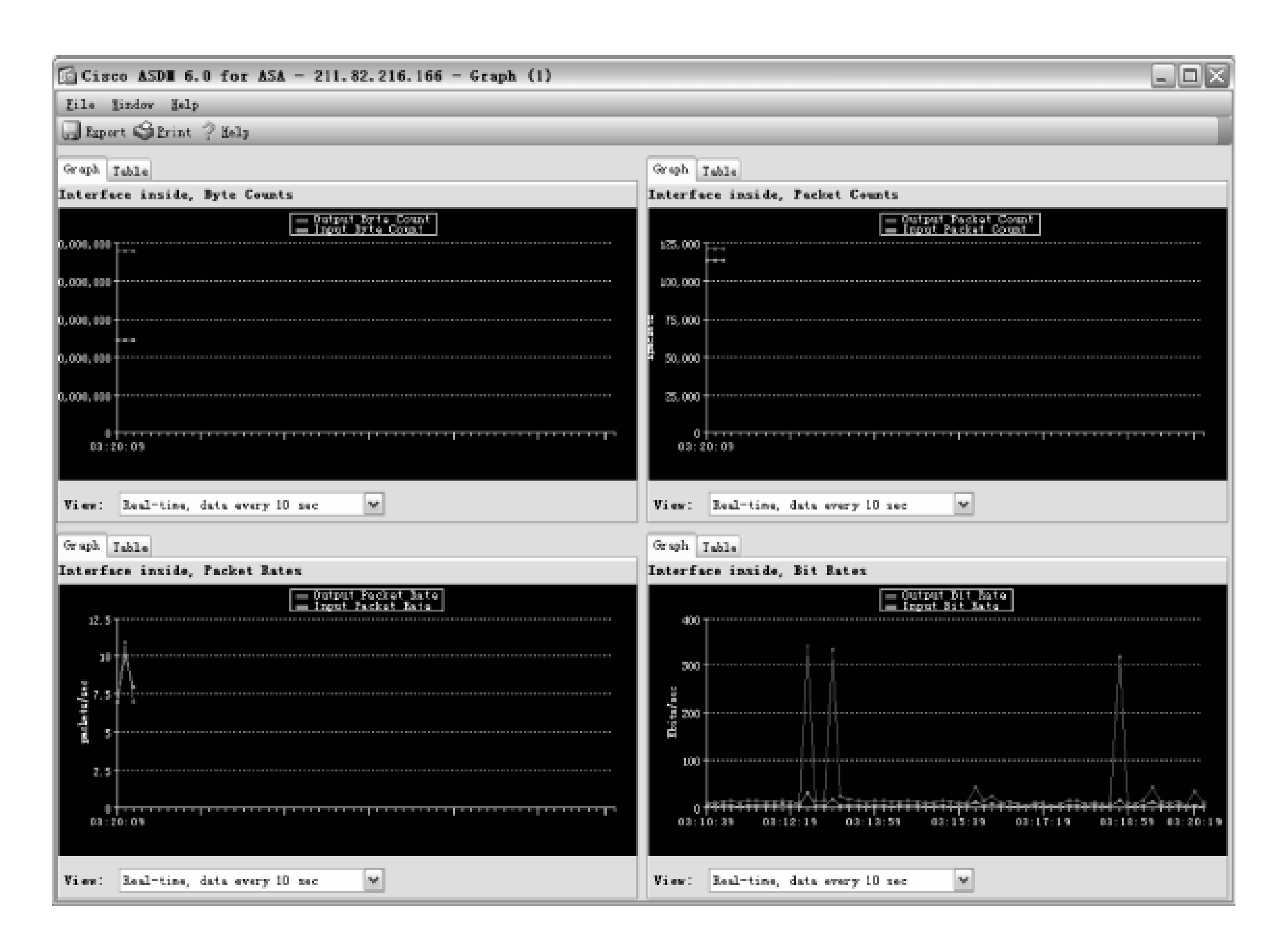


图 10-60　网络流量

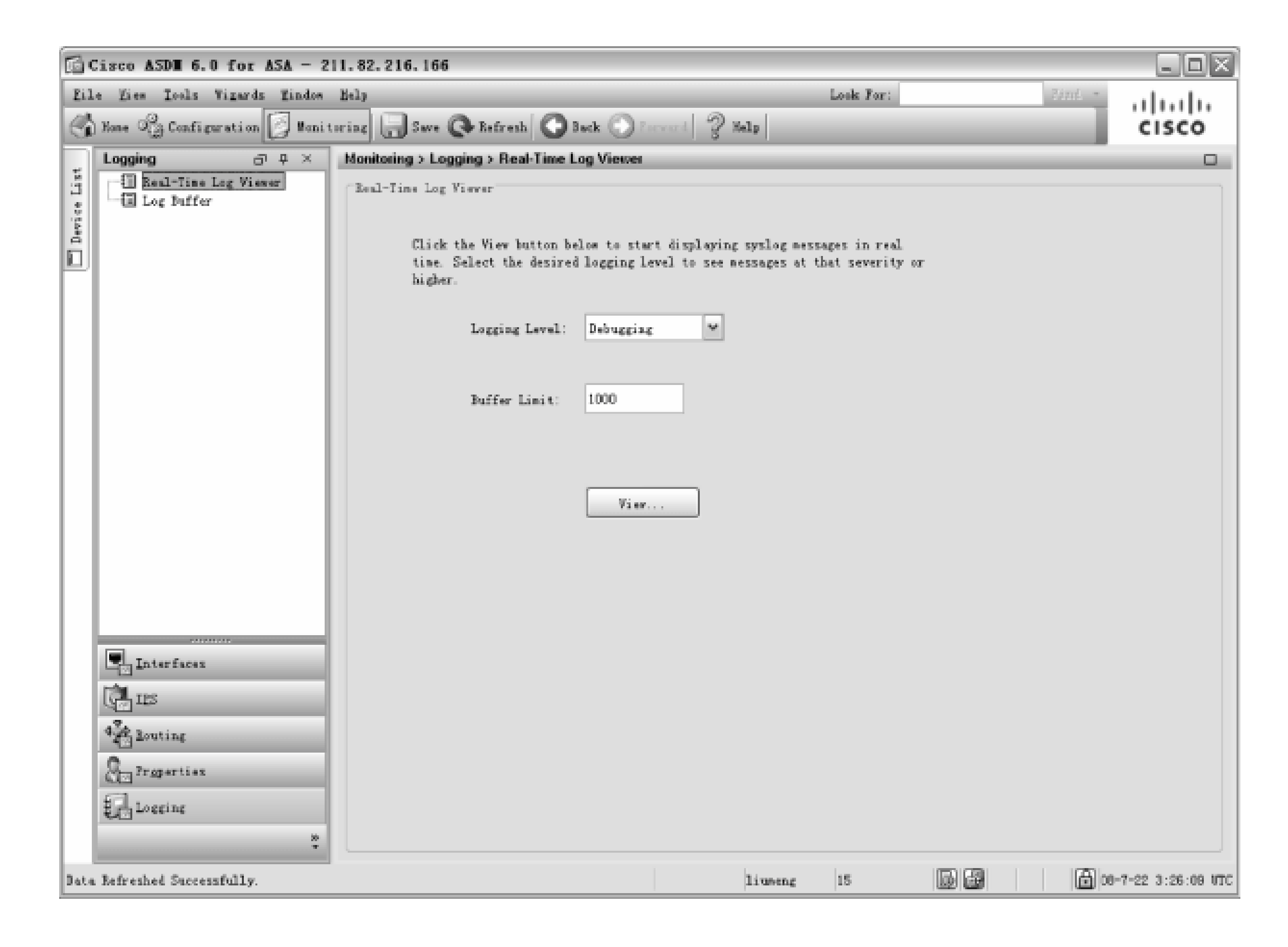


图 10-61　Real-Time Log Viewer 对话框

② 单击 View 按钮，系统日志以视图方式显示，如图 10-62 所示。

图 10-62 系统日志

10.4 客户端安全管理

随着网络用户数量的不断增加，由此而引发的网络安全问题也不断增长，尤其是网络滥用导致的网络拥塞和蠕虫病毒泛滥导致的性能下降，以及系统漏洞导致的恶意攻击问题，如果不采取相应的、有力的应对措施，那么，网络瘫痪的情形将会不断上演。

10.4.1 锁定计算机

所谓锁定计算机是指用户暂时离开但不希望关闭计算机时，锁定计算机工作状态，使其他未授权用户无法登录系统。当解除锁定并重新登录到系统后，打开的文件和正在运行的应用程序仍可以立即使用。需要注意的是，计算机锁定功能仅适用于已设置登录密码的用户账户。受密码保护的屏幕保护程序，可以防止其他用户在当前用户离开时查看屏幕信息并使用计算机。

1. “开始”菜单中的锁定按钮

快速锁定计算机是 Windows Vista 系统的新增功能之一。任意用户登录系统后，单击“开始”菜单，并选择“锁定该计算机”按钮，如图 10-63 所示，即可快速锁定计算机。

2. Win＋L 键

该组合键在 Windows XP 系统中同样适用。离开计算机之前，按 Win＋L 键，即可快速锁定计算机，并显示图 10-64 所示的页面。

3. Ctrl＋Alt＋Delete 键

用户使用任何账户登录 Windows Vista 系统后，按 Ctrl＋Alt＋Delete 键，将显示图 10-65 所示的页面，单击“锁定该计算机”按钮，即可立即锁定当前账户在该计算机的登录状态。

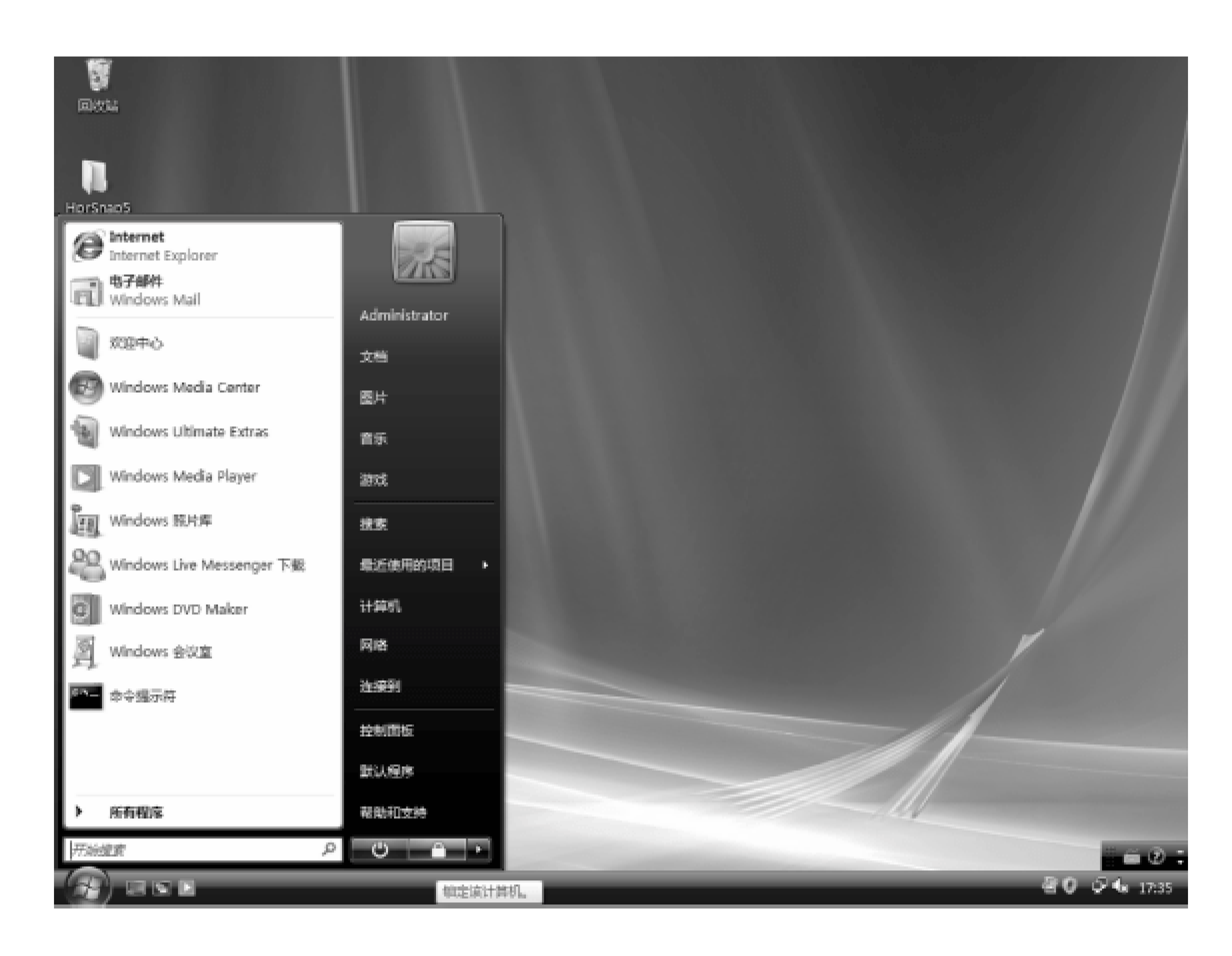


图 10-63　Windows Vista“开始”菜单

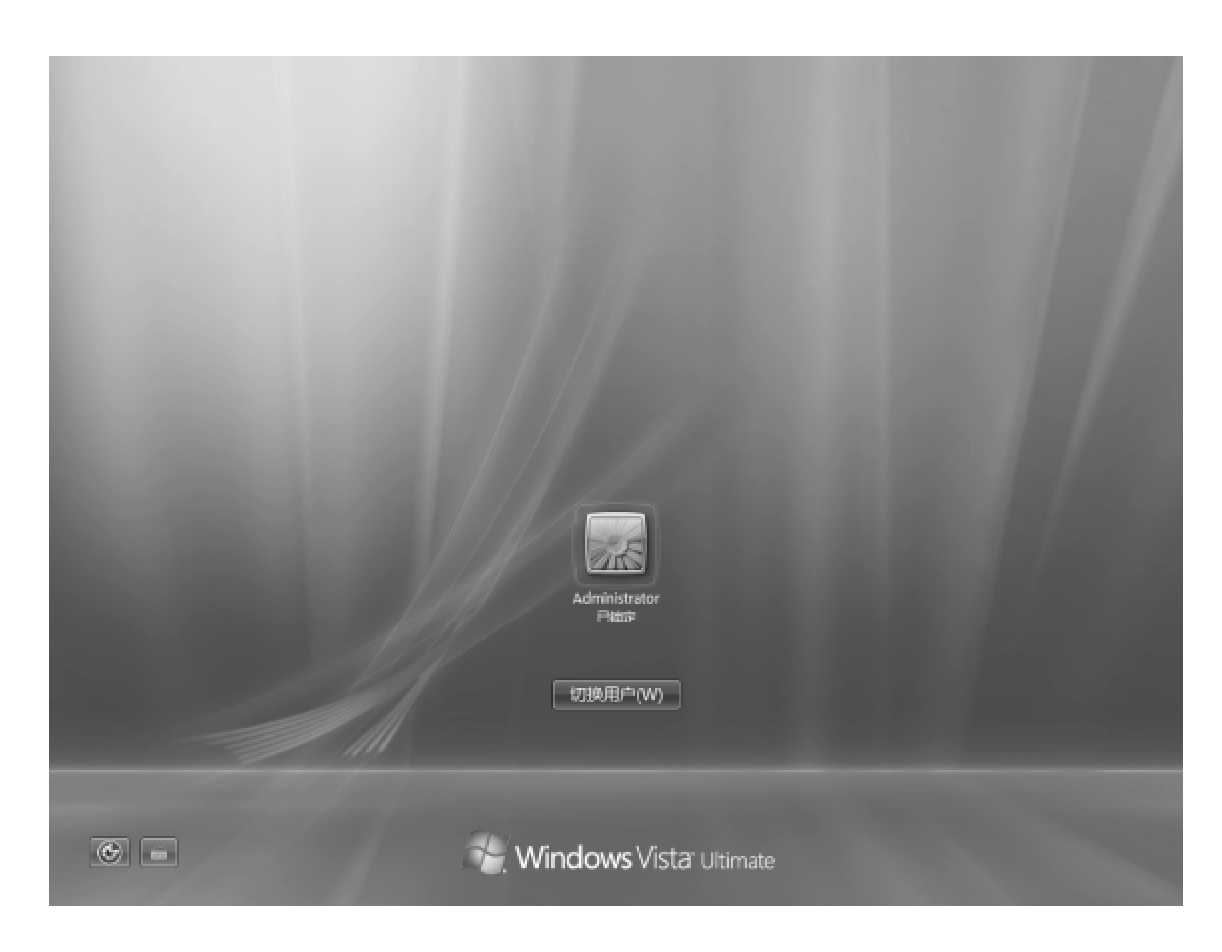


图 10-64　Win+L 键锁定计算机



图 10-65　Ctrl+Alt+Delete 键锁定计算机

提示：*该方法不适用于 Windows XP 系统。*

4. 屏幕保护程序

通过设置屏幕保护程序，可使计算机在指定空闲时间后启动屏幕保护程序并自动锁定计算机，该方式可能存在安全漏洞，建议作为一种备用方法使用，例如，当离开时忘记使用其他方法锁定计算机，则可以通过屏幕保护程序，在一段时间后自动锁定计算机。设置方法如下。

(1) 在桌面空白处右击，选择快捷菜单中的“个性化”命令，打开图 10-66 所示的“个性化外观和声音”窗口。也可以在“控制面板”(经典模式)窗口中，双击“个性化”按钮打开该窗口。

(2) 单击“屏幕保护程序”链接，打开图 10-67 所示的“屏幕保护程序设置”对话框，在“等待”文本框中设置进入屏幕保护程序之前需要等待的时间，默认为 10 分钟。务必选中“在恢复时显示登录屏幕”复选框。




图 10-66 “个性化外观和声音”窗口



图 10-67 “屏幕保护程序设置”对话框

(3) 单击“确定”按钮关闭“屏幕保护程序设置”对话框。这样，在运行屏幕保护程序后，如果通过触动鼠标或按键盘任意键解除屏幕保护程序时，即可显示图 10-68 所示的登录页面，必须输入正确的密码才能登录系统。

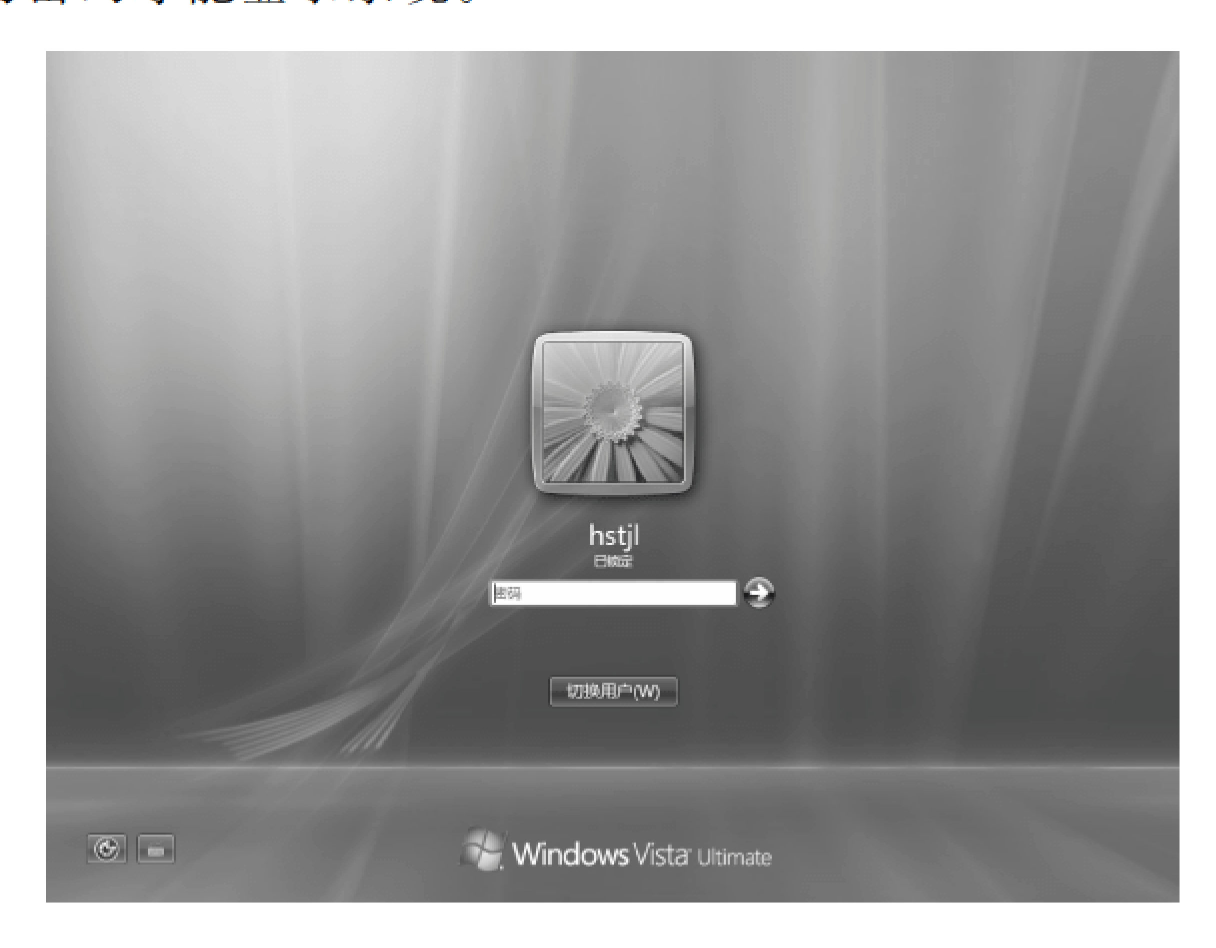


图 10-68 登录页面

提示：上述计算机锁定方式，适用于工作组环境和 Windows 域环境中的所有 Windows Vista 客户端计算机。

10.4.2　保护密码

为了增强计算机的安全性，应该为所有计算机账户设置密码，尤其是对于管理网络和计算机的管理员账户，更应使用具有强保密性的密码。

10.4.3　Windows 防火墙

防火墙有助于防止黑客或恶意软件(如蠕虫)通过网络或 Internet 访问计算机。防火墙还有助于阻止计算机向其他计算机发送恶意软件。因此，防火墙是每个客户端必不可少的安全防护工具。Windows 防火墙是 Windows Vista 系统默认安装的组件之一，并且已经自动开启。Windows Vista 系统防火墙的功能与配置与 Windows Server 2008 类似，用户可通过如下操作启动和配置 Windows 防火墙。

(1) 在“控制面板”窗口中双击“Windows 防火墙”按钮，打开图 10-69 所示的“Windows 防火墙”窗口。系统默认已启用 Windows 防火墙。“网络位置”的显示类型决定了 Windows 防火墙的默认状态，具体设置与 Windows Server 2008 完全相同，此处不再赘述。



图 10-69　“Windows 防火墙”窗口

(2) 单击“更改设置”链接，打开图 10-70 所示的“Windows 防火墙设置”对话框。选中“关闭”单选按钮，即可暂时关闭 Windows 防火墙，但关闭之后系统将失去防火墙保护，更容易遭受黑客和恶意软件攻击。

(3) 选择“例外”选项卡，如图 10-71 所示。在这里同样可以设置允许通过 Windows 防火墙的应用程序或端口，与 Windows Server 2008 完全相同，此处不再赘述。

10.4.4　系统更新设置

微软的 Windows 系统发布后，都会不定时地再发布一些补丁程序，以弥补相应操作系统的漏洞或缺陷。Windows Vista 系统的自动更新设置与 Windows Server 2008 类似，默认都是未配置的，用户可根据实际需要选择是否启用自动更新功能。



图 10-70 “Windows 防火墙设置”对话框



图 10-71 “例外”选项卡

1. 安装更新注意事项

安装系统补丁时，应当注意以下几点。

(1) 安装系统补丁之前切记不要连接网络，尤其是 Internet。所需的补丁程序建议使用其他移动存储设备复制到相应的机器上。如果是在局域网环境，建议搭建一台专用更新服务器(WSUS)，大规模部署之前，先在小范围内进行测试，确认正常后再应用到其他计算机。

(2) 注意某些补丁程序对安装顺序的要求，否则将无法完成安装。

(3) 开始安装补丁程序前应关闭其他应用程序，以免导致安装失败。

(4) 有些补丁程序安装完成后需要重新启动计算机方可生效，应注意及时保存系统状态信息。

(5) 获取补丁程序时应注意其版本要求，如操作系统类型、版本、系统语言等。

(6) 安装过程中如需确认或更改安装目录的，建议保持系统默认设置。

2. 配置 Windows 自动更新

配置 Windows 自动更新功能之前，系统将无法自动获取并安装更新补丁，只能通过移动存储介质或局域网连接，通过其他途径获得的系统补丁手动安装到目标计算机。为提高系统安全性，建议启动 Windows 自动更新功能并确保能够正常连接到 Internet 或内部网络的自动更新服务器。

(1) 在“控制面板”窗口中双击 Windows Update 按钮，打开图 10-72 所示的 Windows Update 窗口，此时尚未启动自动安装更新功能。Windows Ultimate Extras 是针对 Windows Vista Ultimate 提供的程序、服务和收费内容，可以为所有合法用户提供访问独占程序和服务的权限。通过 Windows Ultimate Extras，用户可以获得以下内容。

① 最尖端的应用程序。使用只在 Windows Ultimate Extras 上才可使用的 Microsoft 应用程序，如果有新的下载可用，Windows Update 将会及时通知用户。

② 创新的服务。从独特的服务中受益，这些服务可以定制最适合用户的数字生活方式的新体验，旨在提高用户效率和个性化水平。

③ 独特的发布。下载并侧重于数字生活方式的收费内容，发现有助于当前系统的安全和技巧策略。

(2) 单击“立即启用”按钮，即可按照 Windows 推荐的方式启动自动更新功能，即自动

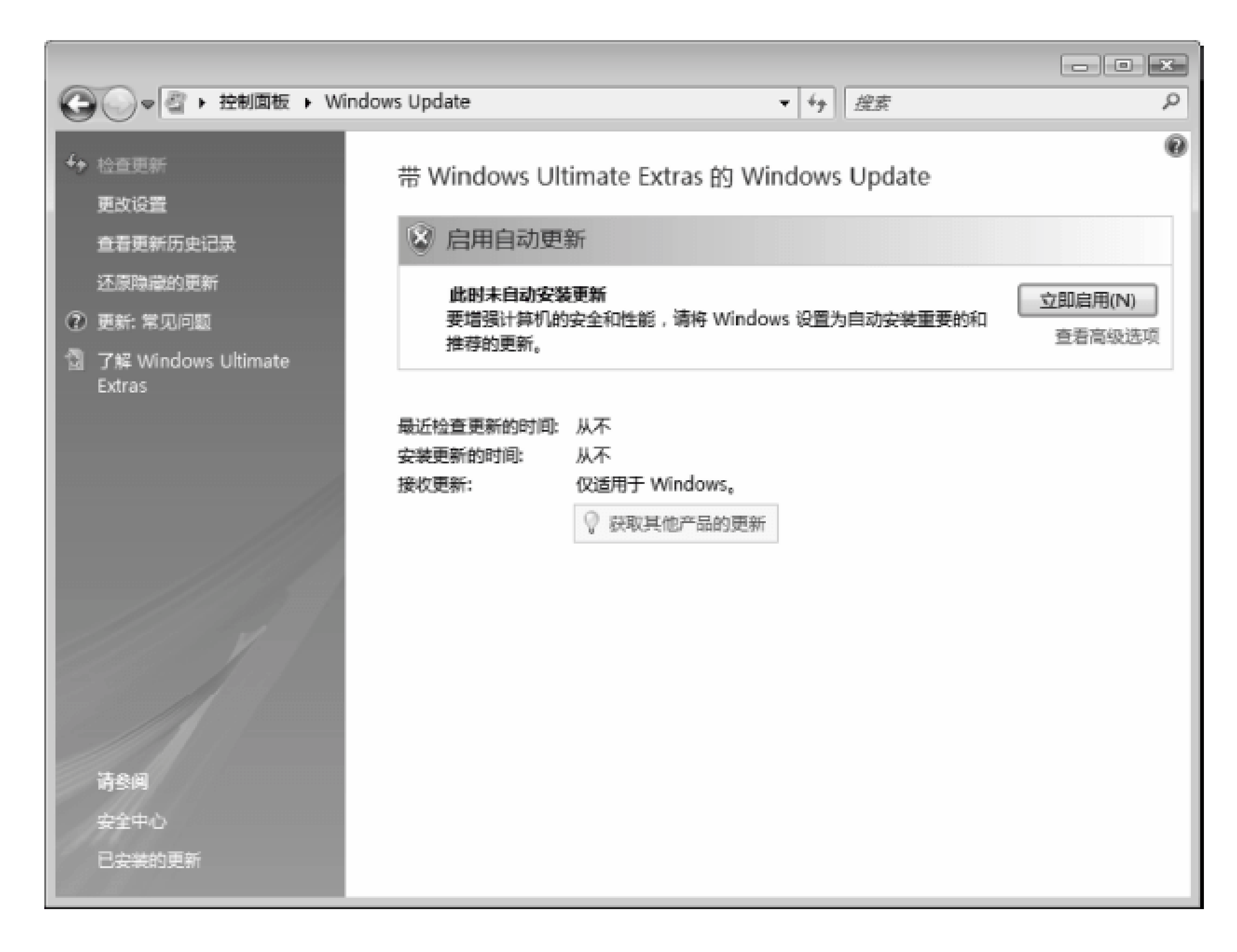


图 10-72　Windows Update 窗口

检查更新，并在每天 3:00 自动安装新的更新，如图 10-73 所示。

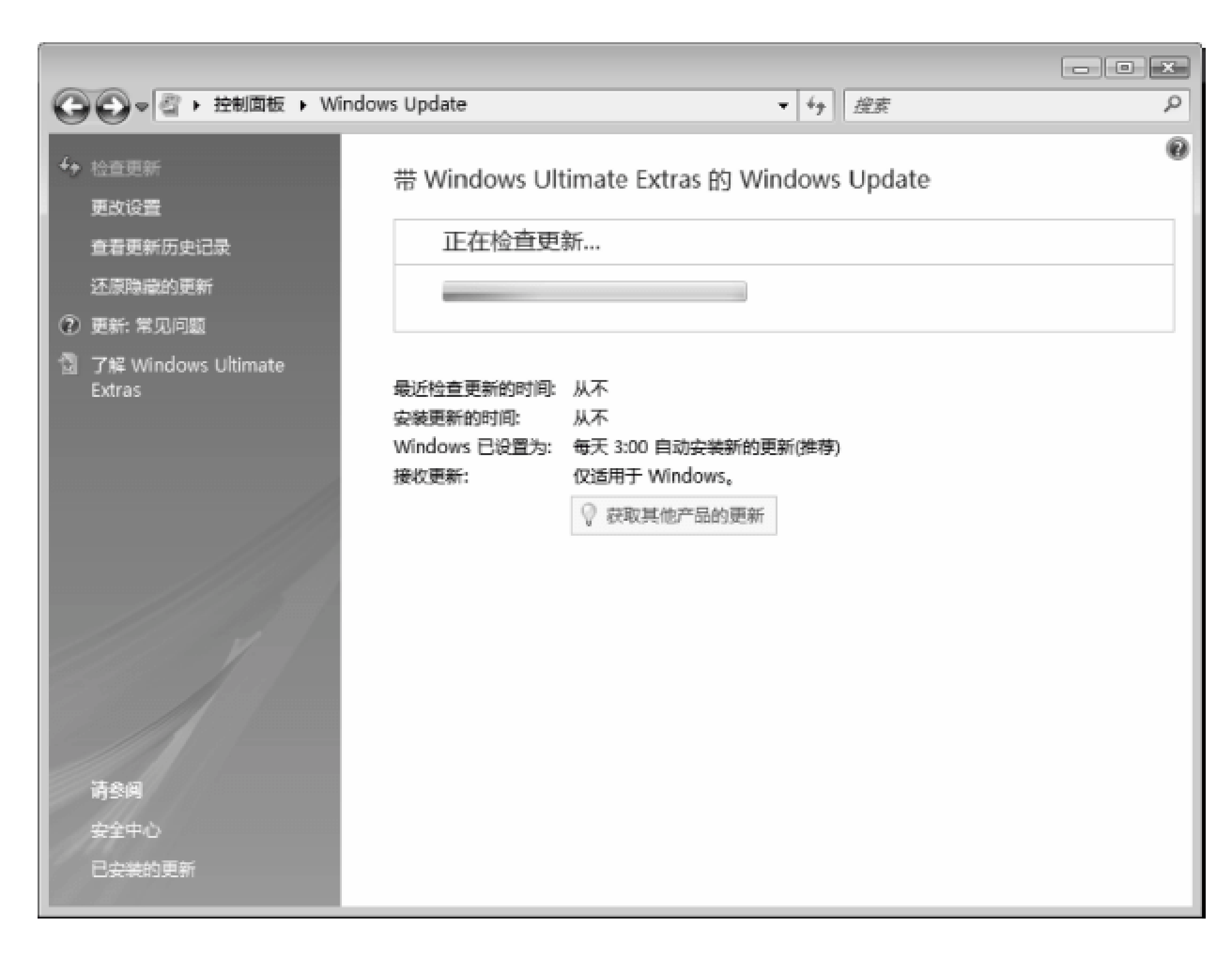


图 10-73　正在检查更新

(3) 如果不希望使用这种方式，则可以单击“更改设置”链接，或者在 Windows Update 窗口中单击“立即启用”按钮下方的“查看高级选项”链接，打开图 10-74 所示的“选择 Windows 安装更新的方法”窗口。建议选中“检查更新，但是让我选择是否下载和安装更新”单选按钮。各种安装方式的具体含义如下。

① 自动安装更新(推荐)：服务器连接到 Internet 后，系统将自动检测 Microsoft Update 服务器是否有所需更新，如果有则将自动下载并安装这些更新。选中该单选按钮后还需要指定系统自动安装更新的具体时间。

② 下载更新，但是让我选择是否安装更新：仅下载所需的系统更新，完成后通知用户在合适的时间手动安装。

③ 检查更新，但是让我选择是否下载和安装更新：仅检测 Microsoft Update 服务器上



图 10-74 “选择 Windows 安装更新的方法”窗口

提供的更新项目，并以列表方式提示系统管理员，管理员可以根据实际情况选择需要下载的系统更新。建议使用这种方式，可以减少不必要的服务器资源和网络带宽浪费。

④ 从不检查更新(不推荐)：关闭系统更新功能，建议不要选中此单选按钮。

(4) 单击“确定”按钮，保存设置即可。

3. 安装系统更新

如果没有将系统更新设置为自动安装，则当服务器上有新的可用更新时，系统托盘将出现“现在有新的更新”提示信息，单击此提示信息即可打开 Windows Update 窗口，在这里用户即可查看和配置将要安装的更新内容。

(1) 单击“现在有新的更新”提示信息，或依次选择“开始”→“所有程序”→Windows Update 命令，打开图 10-75 所示的 Windows Update 窗口。在“下载和安装计算机的更新”选项区域显示了可用更新的数量及大小。

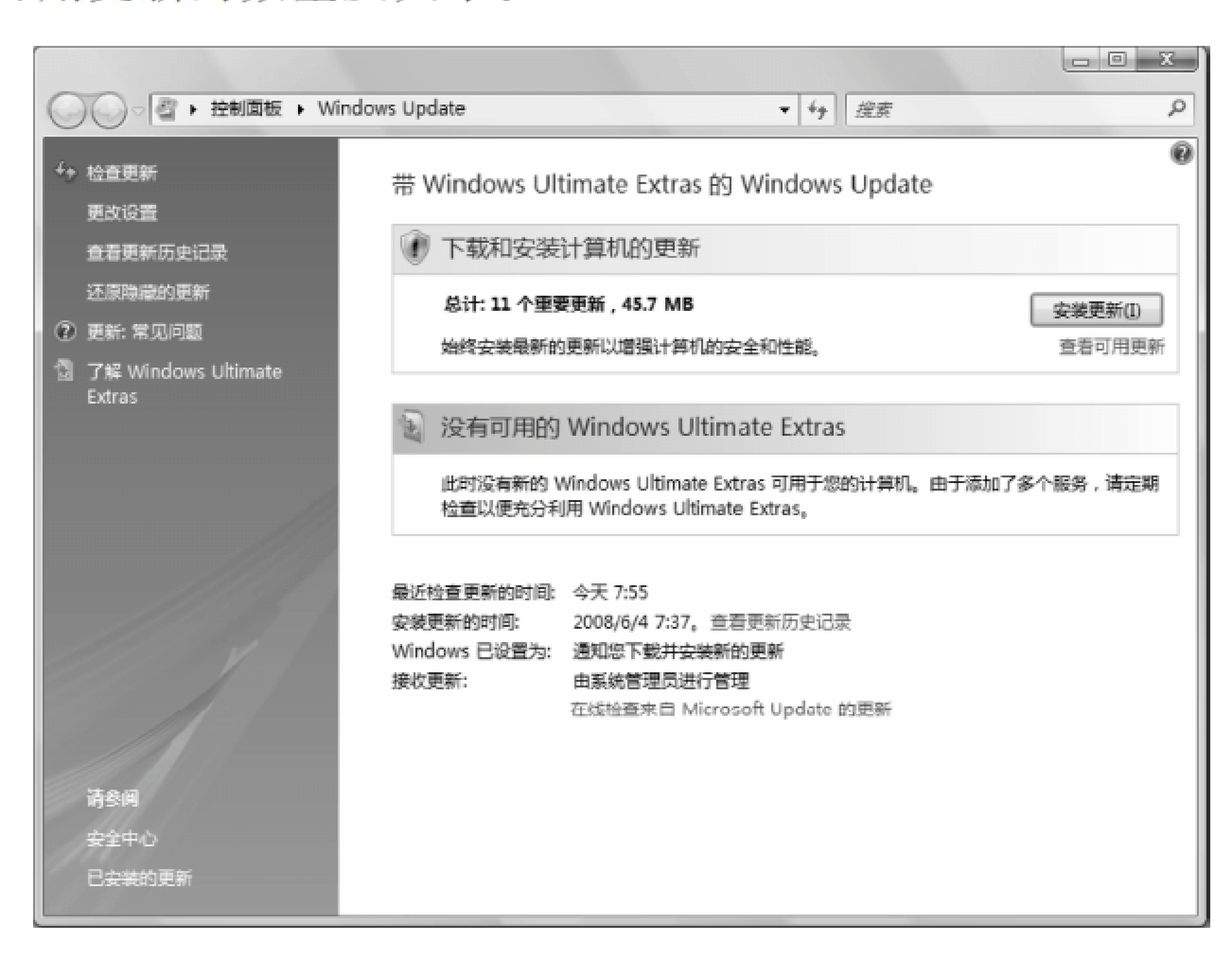


图 10-75 Windows Update 窗口

(2) 单击“查看可用更新”链接，显示图 10-76 所示的“查看可用更新”窗口，在“选择希望安装的更新”列表中，选中其前面的复选框，即表示此次安装该更新，如果取消选中，则表示不安装，但 Windows Update 下次仍会提示安装该更新。



图 10-76　“查看可用更新”窗口

(3) 如果不希望每次都提示没必要安装的系统更新，则可以右击更新名称并选择快捷菜单中的“隐藏”命令将其隐藏，如图 10-77 所示。隐藏之后，更新名称将呈灰色显示，必要时用户还可以从隐藏更新列表中将其恢复。



图 10-77　隐藏不希望安装的更新

(4) 单击“安装”按钮，即可下载并安装选定的系统更新，如图 10-78 所示。本案例中使用的是“检查更新，但是让我选择是否下载和安装更新”方式，所以需要先从服务器下载，然后才会开始安装。

(5) 安装完成后，显示图 10-79 所示的窗口，成功安装了更新。单击“立即重新启动”按钮，重新启动计算机即可应用更新。

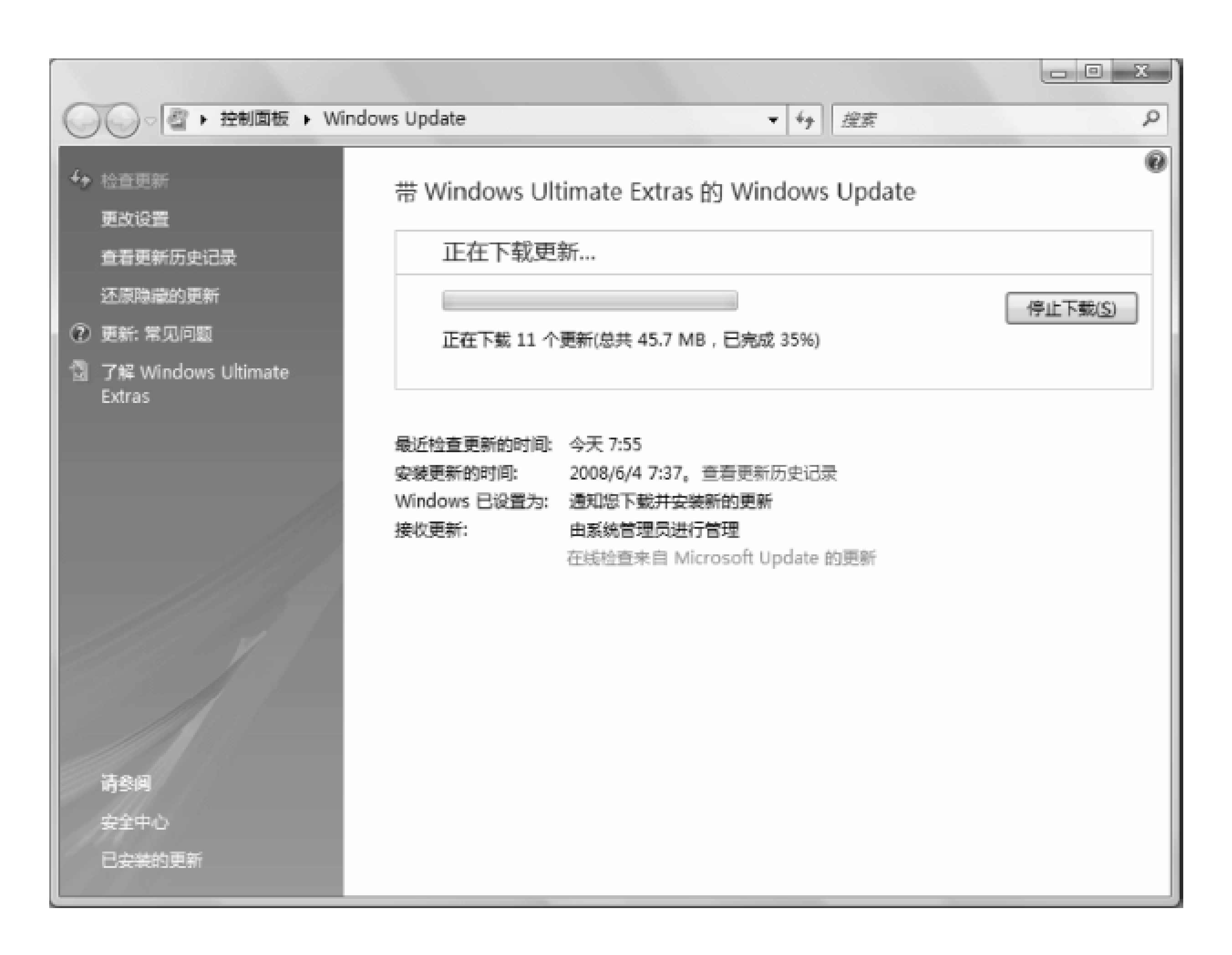


图 10-78　下载并安装更新

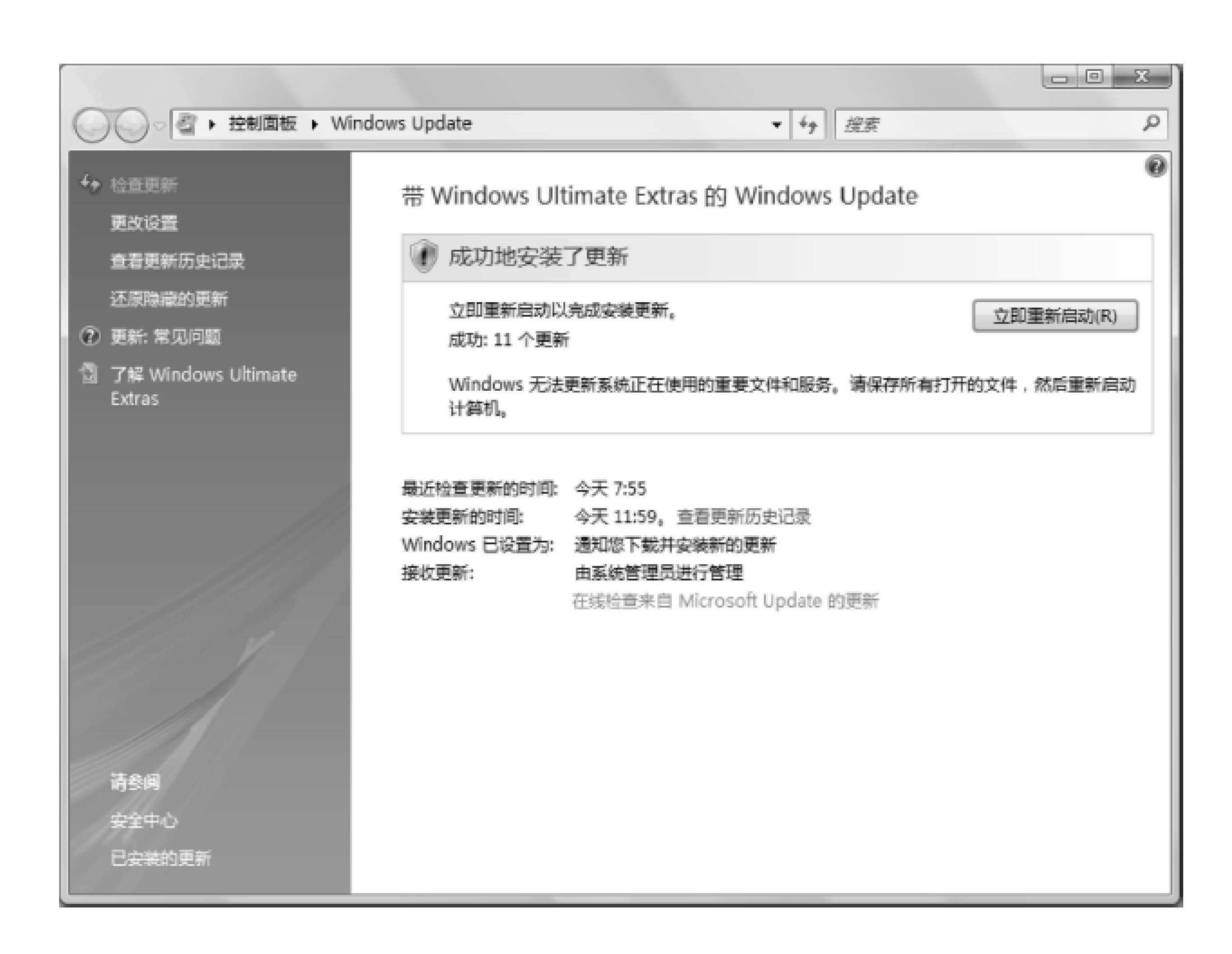


图 10-79　成功安装了更新

习题

1. 交换机的安全管理包括哪些内容?
2. 路由器的安全管理包括哪些内容?
3. Cisco ASDM 具有哪些特点?

实验：使用 Cisco ASDM 配置安全设备

实验目的：

掌握使用 Cisco ASDM 可配置安全设备的内容及配置方法。

实验内容：

配置网络的 DMZ 区域，配置 VPN 远程访问，并使用 Cisco ASDM 监视安全设备。

实验步骤：

(1) 使用 Cisco ASDM 登录安全设备。

(2) 配置 DMZ。

(3) 配置 IPsec VPN 远程访问。

(4) 配置 Site-to-Site VPN 远程访问。

(5) 监视安全设备的运行状态。

(6) 查看和分析网络流量。

(7) 查看和分析系统日志。

第 11 章 chapter 11

网络客户端管理

客户端计算机是网络的重要组成部分，是企业人员日常工作所使用的工作平台。对于使用客户端计算机的用户而言，有可能由于安全意识不足或系统漏洞等原因造成客户端计算机的故障，此时则会对用户的工作造成直接的影响。

11.1　网络客户端管理规划

在当前网络中，主要包括两种客户端操作系统，分别为 Windows XP 和 Windows Vista。其中，半数以上的客户端使用的是 Windows XP 操作系统。

11.1.1　项目背景

客户端计算机主要是网络中的普通用户所使用的计算机，因为并不是所有的用户都具有安全意识，所以，相对于有专人维护安全的服务器而言，客户端计算机更容易成为攻击对象，因此客户端的安全也是管理员的重要工作之一。

另外，为了能够达到统一管理的目的，在当前网络中，要求所有客户端计算机均加入到域中，从而可以在服务器端进行统一的管理，无论是客户端的系统管理还是安全管理均可实现。

11.1.2　项目需求

在该项目中，因为大部分客户端的位置比较固定，其采用双绞线方式接入网络，而对于位置经常变换的客户端而言则采用无线方式接入网络。对于客户端的管理，首先必须保证客户端的系统安全，才能使客户端计算机更好地完成其任务；另外，需要企业内的所有客户端使用相同的工作环境，安装统一软件。

11.1.3　解决方案

鉴于在该项目对客户端管理的要求，可通过如下各项方案实现。

（1）为了提高客户端计算机的安全性，微软会不定期地发布系统补丁，对于这些补丁程序，客户端计算机应该在补丁发布后尽快安装。这是因为在系统补丁发布后，到客户端安装这些补丁程序期间，客户端是最危险的。所以，必须在微软发布补丁后及时安装。另外，虽然现在网络提供商所提供的网络带宽越来越宽，但如果让网络中所有客户端自行下载，其占用的网络带宽也是非常大的，所以在当前网络中，通过安装 WSUS 服务器，统一下载补丁程

序，并使用组策略方式，将 WSUS 服务器的地址发布到所有客户端计算机上，实现所有客户端计算机的补丁程序的安装。

（2）可以通过组策略的方式解决客户端使用相同工作环境的问题，通过在域控制器上设置组策略，可以配置客户端的 IE 浏览器标题、IE 浏览器主页等内容。

（3）防火墙的作用是拦截非法连接，从而保证计算机的安全。为了保证计算机的安全，客户端必须启用防火墙功能。通过在域控制器上配置组策略，强制客户端计算机启用 Windows 防火墙。

（4）对于安装统一软件的要求，同样也可能通过组策略方式实现。使用组策略可以轻松地将 MSI 文件分发到客户端计算机上，而对于 EXE 文件，则需要使用发布 ZAP 文件的方式进行分发。

11.2 系统更新管理

WSUS(Windows Software Update Service)作为微软为数不多的免费服务程序，允许管理员在 Windows 工作站和服务器上快速、可靠地部署重大更新和安全更新。具体关于 WSUS 的安装和配置，参见其他相关资料，这里就不再赘述。为了使网络中的客户端可以从 WSUS 服务器上获得更新，需要对其进行相关的设置。在域网络环境，通常情况下，建议使用组策略方式将 WSUS 服务器地址分发到客户端计算机上。

11.2.1 通过组策略编辑器配置

如果通过组策略为 Active Directory 网络中的计算机指定 WSUS 升级服务器的地址，需要在包括网络中所有计算机的“组织单元”或其上一级“组织单元”配置组策略，或者将需要更新的计算机“移动”到一个新创建的“组织单元”中，然后再对该组中的所有计算机进行操作即可，具体步骤如下。

（1）新建一个用于保存所有 WSUS 3.0 客户端计算机的组织单位，也可以使用 AD 默认提供的组织单位。使用新建计算机的方法将客户端计算机添加到指定的组织单位中，也可以从其他组织单位中直接添加。

（2）依次选择“开始”→“管理工具”→“组策略管理”命令，显示图 11-1 所示的“组策略管理”窗口，依次展开“林：coolpen.net”→“域”→coolpen.net 目录。

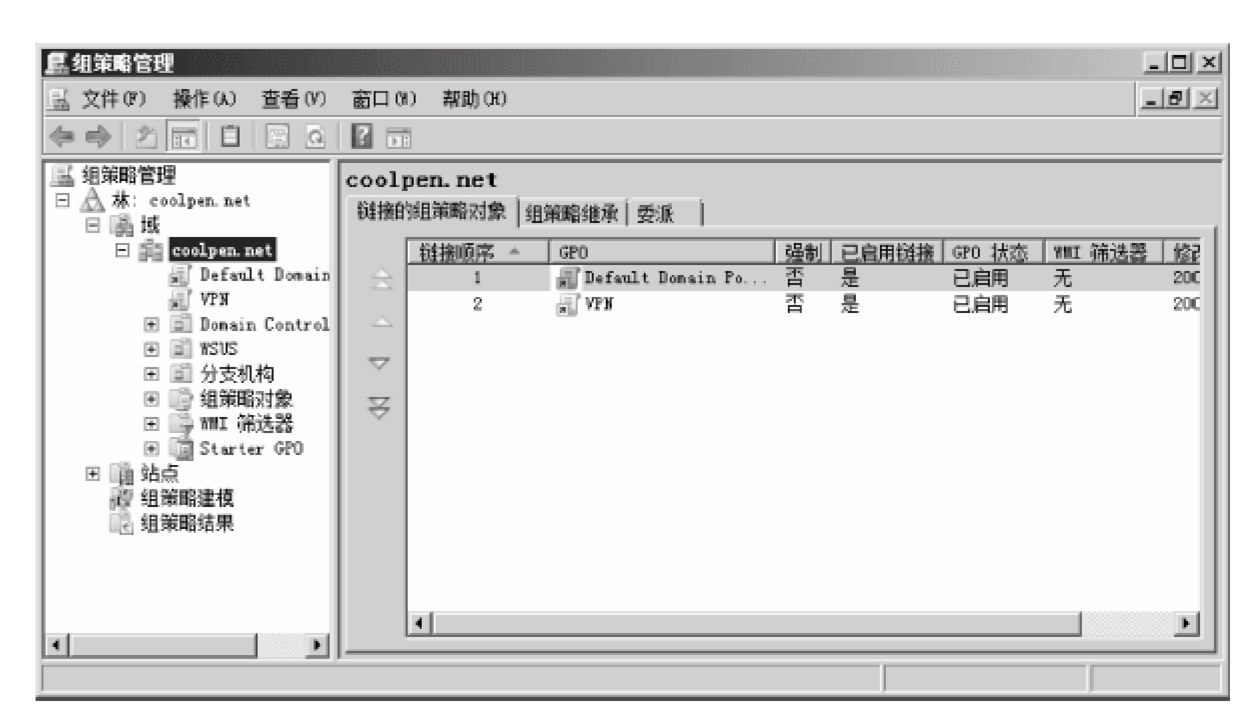


图 11-1 “组策略管理”窗口

(3) 右击组织单位并选择“在这个域中创建 GPO 并在此处链接”命令，显示图 11-2 所示的“新建 GPO”对话框。在“名称”文本框中输入想要创建的组策略名称。

(4) 单击“确定”按钮，返回“组策略管理”窗口。然后右击新建的组策略，在快捷菜单中选择“编辑”命令，打开“组策略管理编辑器”窗口，并依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→Windows Update 目录，即可看到所有的设置选项，默认都是未配置的。

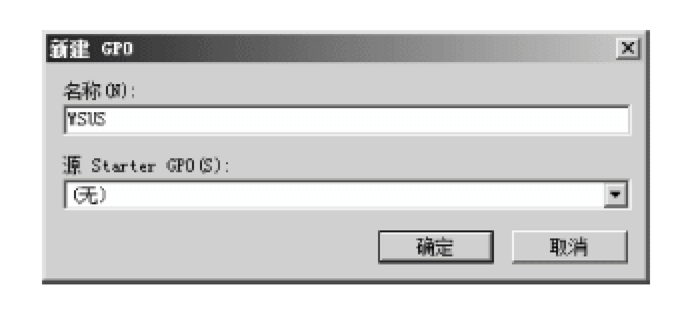


图 11-2 “新建 GPO”对话框

(5) 双击“配置自动更新”链接，打开图 11-3 所示的“配置自动更新 属性”对话框。首先选中“已启用”单选按钮激活下面的选项，然后在“配置自动更新”下拉列表框中选择对应的自动更新类型，共有 4 种类型，这里选择“4-自动下载并计划安装”选项，即自动下载更新并计划安装，还要继续设置“计划安装日期”和“计划安装时间”选项，指定执行安装的日期和时间。设置完成后单击“应用”和“确定”按钮保存设置。

(6) 双击“指定 Intranet Microsoft 更新服务位置”链接，打开图 11-4 所示的“指定 Intranet Microsoft 更新服务位置 属性”对话框。首先选中“已启用”单选按钮，然后在“设置检测更新的 Intranet 更新服务”文本框中，输入网络中的 WSUS 3.0 服务器地址，在“设置 Intranet 统计服务器”文本框中，输入用于获取客户端状态信息的服务器地址。设置完成后，单击“确定”按钮，保存设置即可。

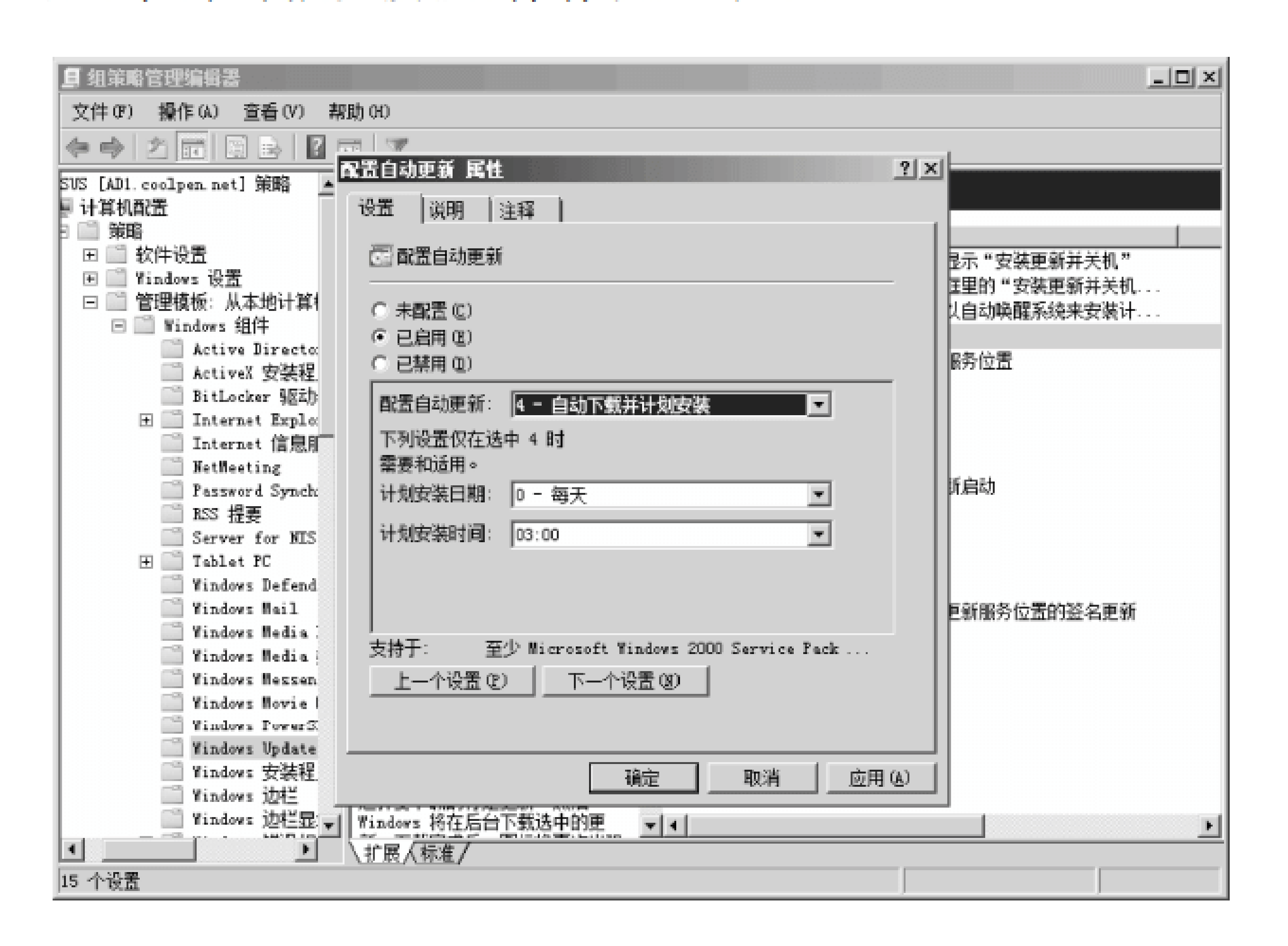


图 11-3 启用自动更新功能

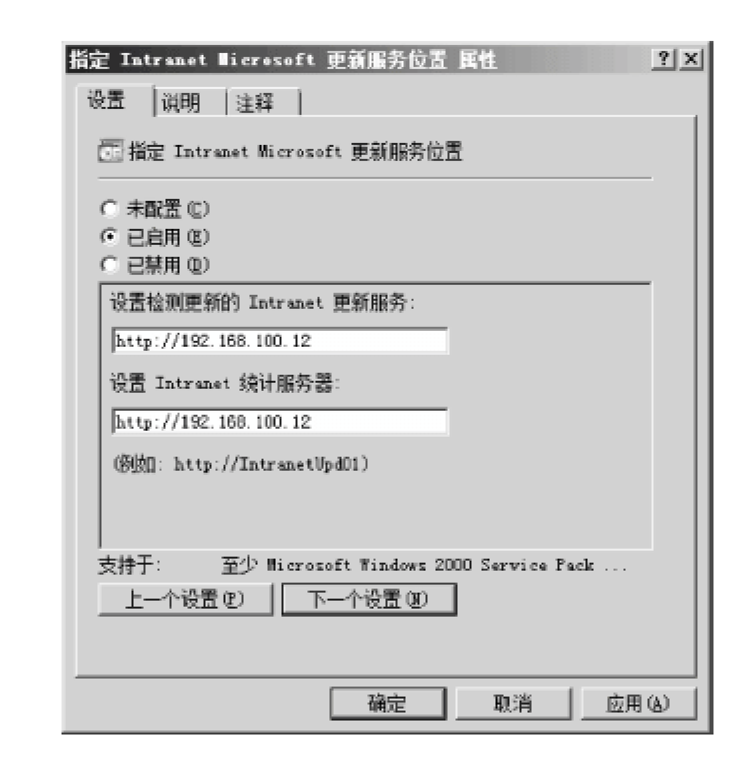


图 11-4 “指定 Intranet Microsoft 更新服务位置 属性”对话框

需要注意的是，由于组策略的刷新和应用需要一定的时间，所以保存编辑结果后即使客户端重新登录域控制器也可能无法立即联系到 WSUS 服务器。而默认情况下，每隔 90 分钟计算机组策略便会在后台刷新一次，刷新的时间可能随机偏移 0～30 分钟，客户端计算机要在域控制器刷新组策略 20 分钟后才可以应用到组策略。如果想要以更快的速度刷新组策略，可以在服务器端设置组策略后，通过运行 gpupdate 命令让设置即时生效，并在客户端计算机通过运行 gpupdate/force 命令立刻生效。如果计算机不是 Active Directory 的成员，可以通过输入 wuauclt.exe/detectnow 来消除 20 分钟延时。

11.2.2 通过本地策略配置

如果计算机没有加入到 Active Directory，或者想覆盖 Active Directory 中通过组策略指定的 WSUS 升级服务器的地址或配置，可以在客户端计算机上配置本地策略实现。

打开“运行”对话框，输入 gpedit.msc 并按 Enter 键。打开图 11-5 所示的“组策略对象编辑器”窗口，依次展开“计算机配置”→“管理模板”→“Windows 组件”→Windows Update 目录，具体设置方法与在域控制器上设置方法相同，这里就不再赘述。

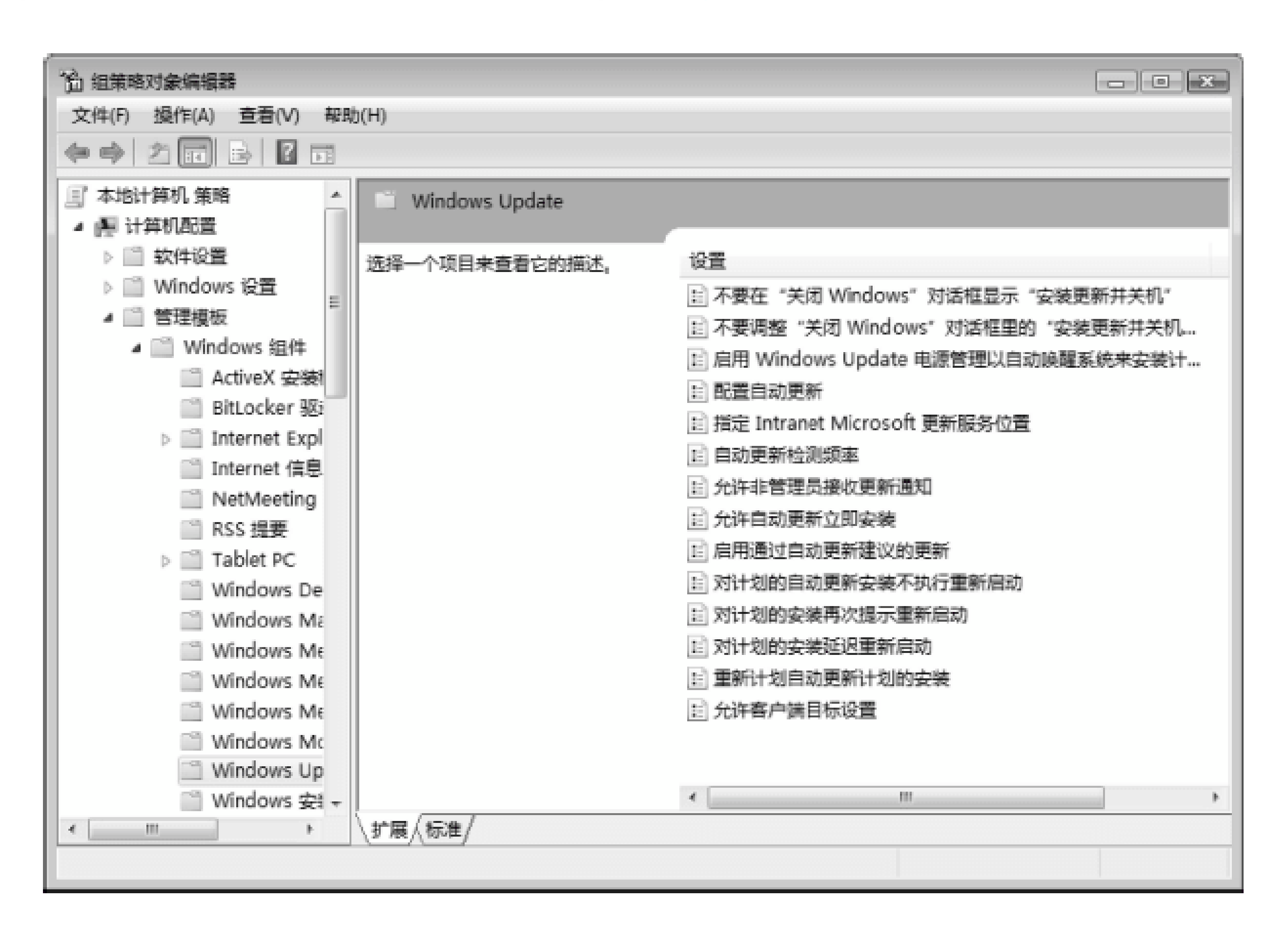


图 11-5 “组策略对象编辑器”窗口

11.3 网络接入管理

客户端接入网络通常包括两种方式，一种是使用双绞线将计算机连接到交换机等网络设备；一种是使用无线网卡接入网络。对于第一种方法，只需使用双绞线将计算机与交换机进行连接即可；而对于第二种方法，则需要分别在无线路由器和客户端计算机上进行设置。这里以 Windows XP 为例介绍客户端计算机接入网络的具体操作。另外，无论采用哪种方式，其设置 IP 地址的方法基本相同，具体内容参见相关资料，这里不再赘述。

11.3.1 Windows XP 客户端配置

当无线网卡驱动程序支持 Windows XP SP2 的“无线自动配置”时，可以通过以下操作配置 Windows XP SP2 的无线网络。

(1) 在 Windows XP SP2 中安装无线网络适配器。这个过程包括为无线网络适配器安装正确的驱动程序，以便在“网络连接”中作为一个无线连接出现。

(2) 当计算机在家庭或小型企业的无线 AP 范围内时，Windows XP 应该检测到网络信号，如图 11-6 所示，并在任务栏的通知区域显示“检测到无线网络”提示消息。

(3) 单击该提示消息，显示图 11-7 所示的带有无线连接名称的对话框。如果没有看到通知，在“网络连接”中右击无线网络适配器，然后单击“查看可用的无线连接”按钮，也可显示该对话框。

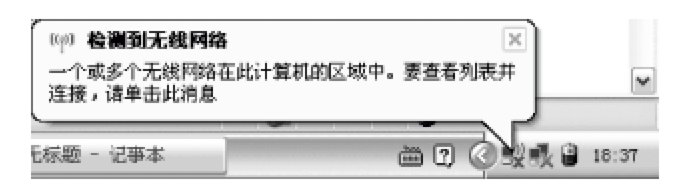


图 11-6 提示检测到无线网络



图 11-7 可用的无线连接

(4) 双击无线网络名称，Windows XP 将尝试连接到该无线网络。

(5) 由于 Windows XP 还没有配置用于该无线网络的 WEP 加密密钥，连接尝试将会失败，Windows XP 将使用一个"无线网络连接"对话框发出提示，如图 11-8 所示。在"网络密钥"和"确认网络密钥"中输入 WEP 密钥，然后单击"连接"按钮。

(6) 如果在"选择无线网络"对话框中，无线网络的状态消息是"已连接上"，如图 11-9 所示，那么连接就成功了。



图 11-8 提示输入 WEP 密钥



图 11-9 无线网络连接成功

(7) 如果"选择无线网络"对话框中无线网络的状态消息是"身份验证没有成功"，则应当在"相关任务"列表中单击"更改首选网络的顺序"按钮，打开"无线网络 属性"对话框，选择"无线网络配置"选项卡，在"首选网络"列表中单击无线网络名称，然后单击"属性"按钮，显示图 11-10 所示的该无线连接属性对话框。

(8) 在"网络验证"下拉列表框中选择"开放式"选项。在"数据加密"下拉列表框中选择 WEP 选项。在"网络密钥"和"确认网络密钥"文本框中，输入无线 AP 上配置的 WEP 加密密钥。在"密钥索引(高级)"中，选择对应于无线 AP 上配置的加密密钥内存位置的密钥索引。

(9) 依次单击"确定"按钮，保存对无线网络和无线网卡的修改。无线客户端与无线 AP 的网络连接正式建立，显示图 11-11 所示的"无线网络 状态"对话框。



图 11-10　无线连接属性对话框



图 11-11　“无线网络 状态”对话框

11.3.2　专用配置程序

如果使用无线网卡自带的配置程序，也可实现与无线 AP 的连接。下面以 TP-Link TL-WN321G 1.0 Utility 为例，介绍无线客户端的设置。

（1）启用配置程序，程序会自动搜索无线 AP 网络，并显示在“无线网络”选项卡的列表框中，如图 11-12 所示。

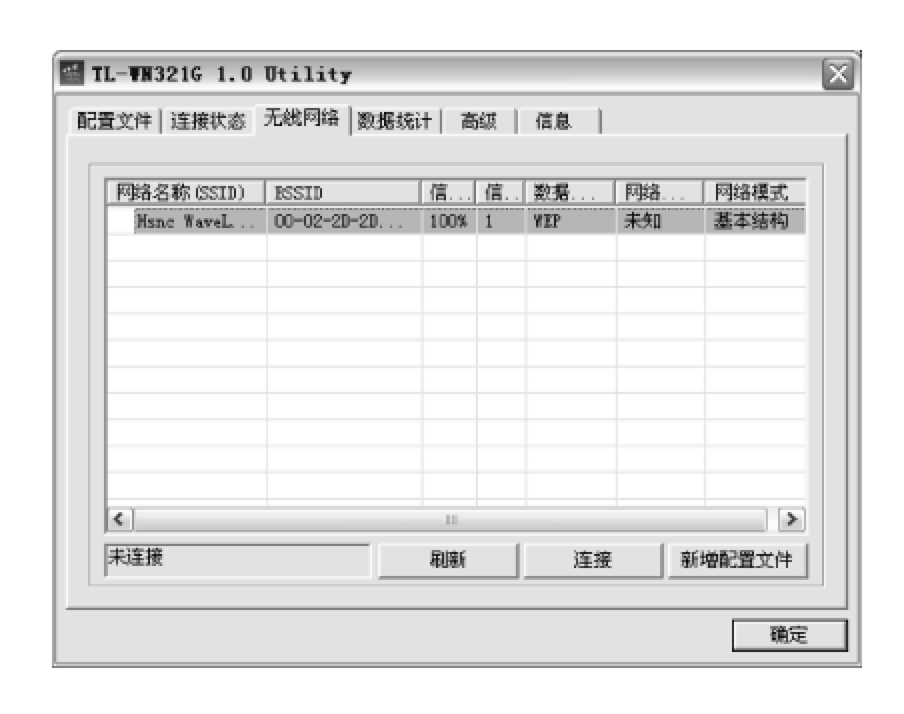


图 11-12　已搜索到的网络

（2）选择无线 AP 网络，单击“连接”按钮，如果无线网络设置了加密，就会显示图 11-13 所示的“身份验证及安全”对话框，要求输入登录密码。在“密钥”下拉列表框中选择 ASCII 选项，并在文本框中输入登录密码，单击“确定”按钮。

（3）选择“连接状态”选项卡，如图 11-14 所示，显示该无线网卡已经连接至无线网络。



图 11-13　“身份验证及安全”对话框



图 11-14　“连接状态”选项卡

11.3.3　迅驰客户端设置

迅驰客户端设置步骤如下。

（1）双击任务栏托盘区的迅驰图标，显示迅驰无线网卡配置程序“英特尔(R) PROSet/

无线”对话框，如图 11-15 所示。系统会自动搜索无线网络，并将所搜索到的网络显示在“无线网络”列表框中。

(2) 选择欲接入的无线网络(如 TP-LINK)，单击“连接”按钮，如果无线网络设置了加密，将显示图 11-16 所示的“连接至：TP-LINK”对话框，需要输入网络密钥才能连接。

(3) 在“无线安全性密码”文本框中输入无线路由器中设置的密钥，单击“确定”按钮即可连接网络，如图 11-17 所示，此时就可与网络中的其他计算机进行连接，并可通过无线路由器连接 Internet 了。如果无线主机没有设置 IP 地址，并且无线路由器启用了 DHCP 服务，则无线主机会自动获取 IP 地址。否则，需要手工为无线客户端设置 IP 地址信息。



图 11-15 迅驰无线网卡配置程序

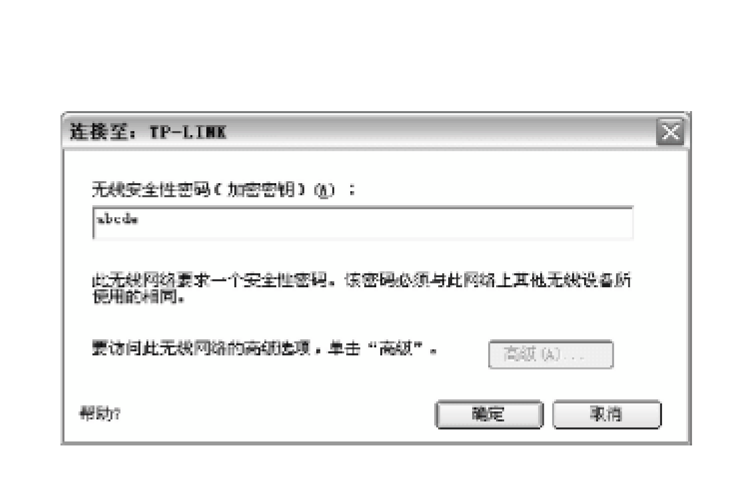


图11-16 “连接至：TP-LINK”对话框

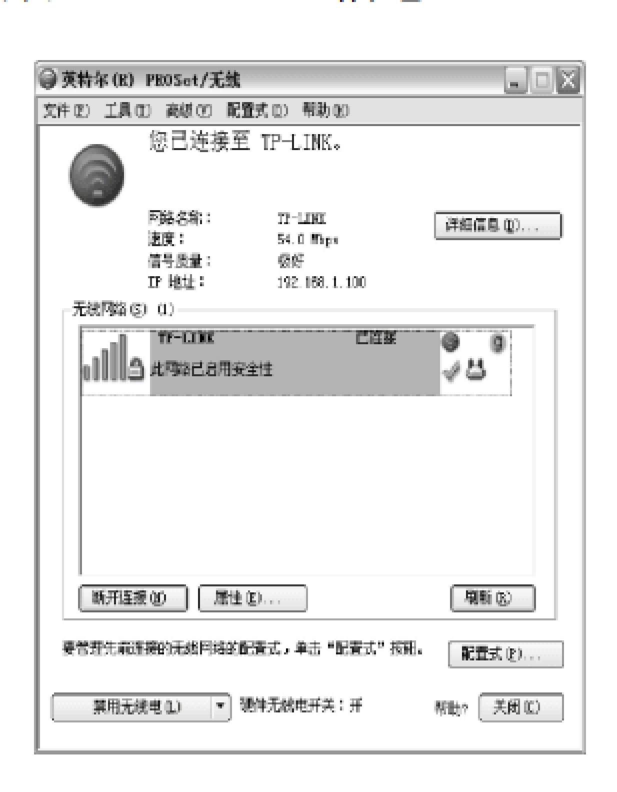


图 11-17 连接无线网络

11.4 组策略管理

在企业网络中，因为存在多台客户端计算机，以及所使用的人员的计算机水平的不同，其管理难度是可想而知的。如果采用传统的管理计算机的方式，显然管理效率是很低的，因此，在企业网络中通常会采用组策略的方式，对网络中的计算机进行统一的管理和配置。

11.4.1 使用组策略定制用户环境

“组策略管理编辑器”包括“计算机配置”和“用户配置”两个选项，在“计算机配置”中进行的设置将应用于编辑的所属组织单位中的“计算机对象”，而在“用户配置”中进行的设置将应用于编辑的所属组织单位中的“用户对象”所登录的计算机。

1. 修改 IE 浏览器的标题

在“组策略管理编辑器”窗口中，依次展开“用户配置”→“策略”→“Windows 设置”→“Internet Explorer 维护”→“浏览器用户界面”目录，如图 11-18 所示。

在右侧双击“浏览器标题”链接，打开“浏览器标题”对话框，如图 11-19 所示。选中“自定义标题栏”复选框，在“标题栏文字”文本框中输入想要在 IE 标题栏显示的文字(如 COOLPEN)，然后单击“确定”按钮返回“组策略管理编辑器”窗口。

2. 自定义主页

在“组策略管理编辑器”窗口中，依次展开“用户配置”→“策略”→“Windows 设置”→

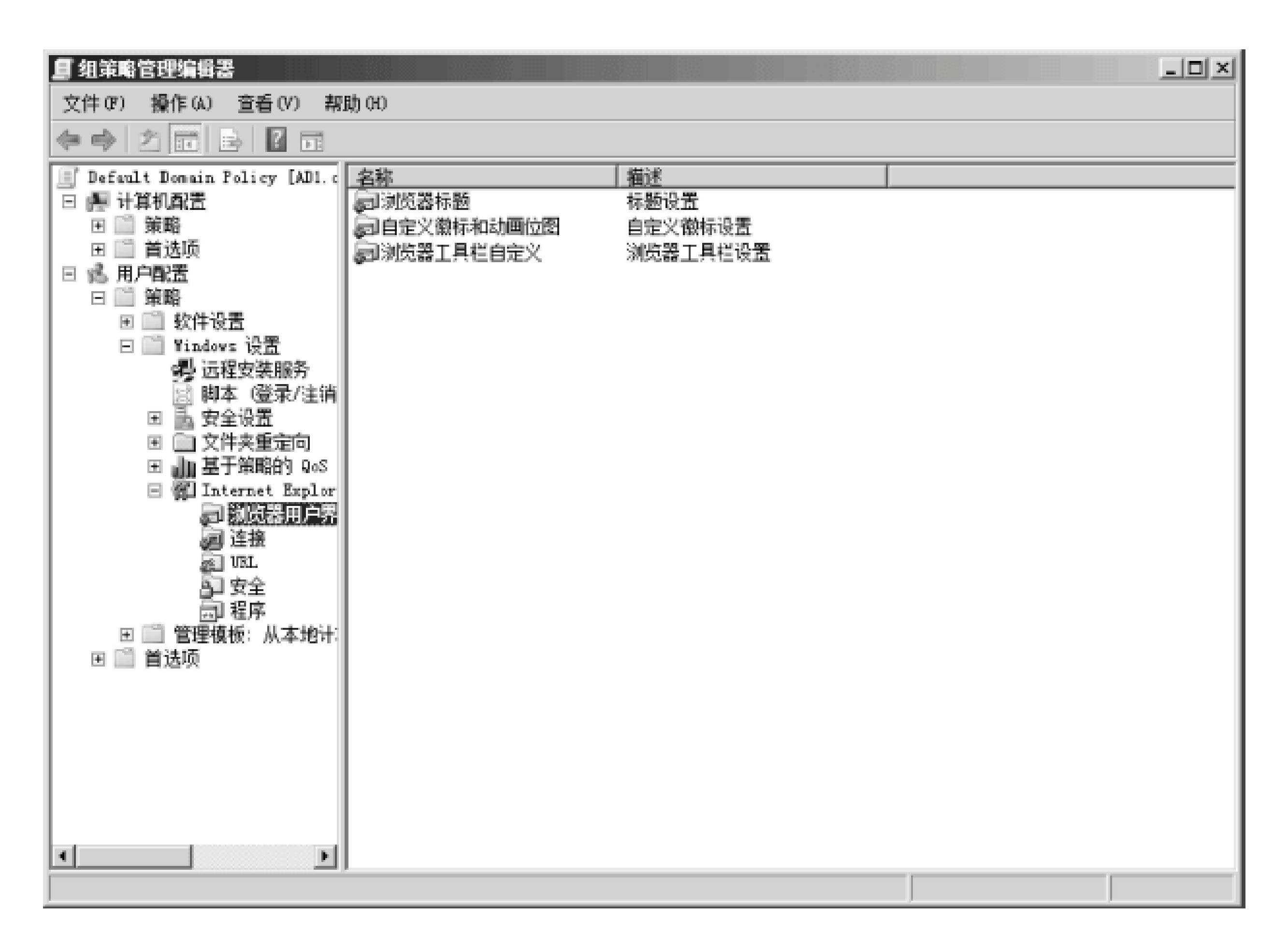


图 11-18　使用组策略对 IE 进行定制

“Internet Explorer 维护”→URL 目录。在右侧双击“重要 URL”链接，显示图 11-20 所示的“重要 URL”对话框。在此有 3 个文本框，分别是“主页 URL”、“搜索栏 URL”和“联机支持页的 URL”。分别选中“自定义主页 URL”、“自定义搜索栏 URL”、“自定义联机支持页 URL”复选框，然后在文本框中输入相应的主页地址即可。需要注意的是，输入的地址必须以“http://”开始。



图 11-19　定义 IE 标题栏

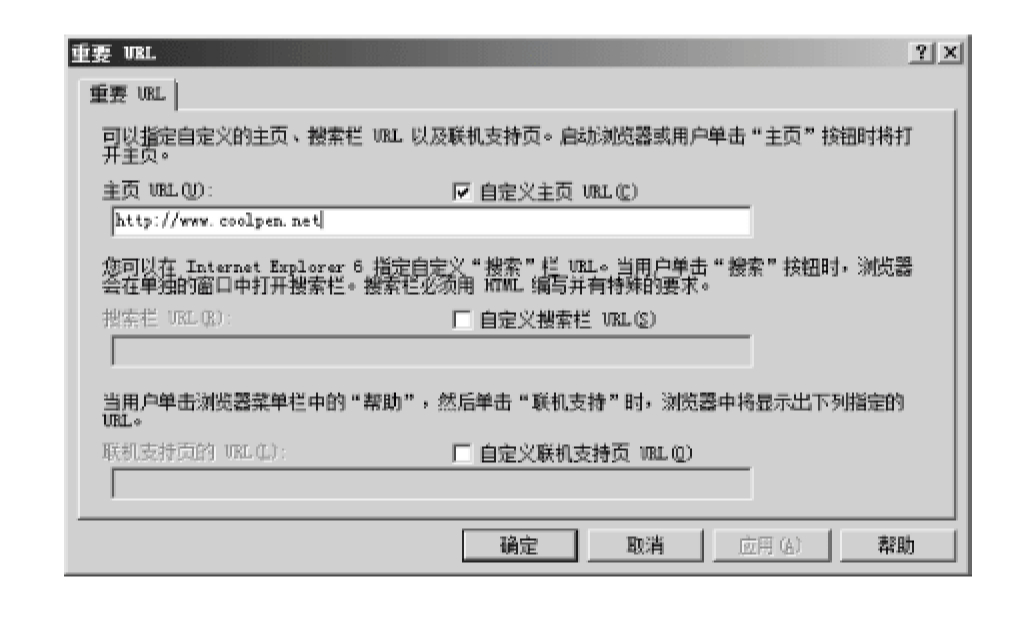


图 11-20　“重要 URL”对话框

3. 修改 Windows 防火墙设置

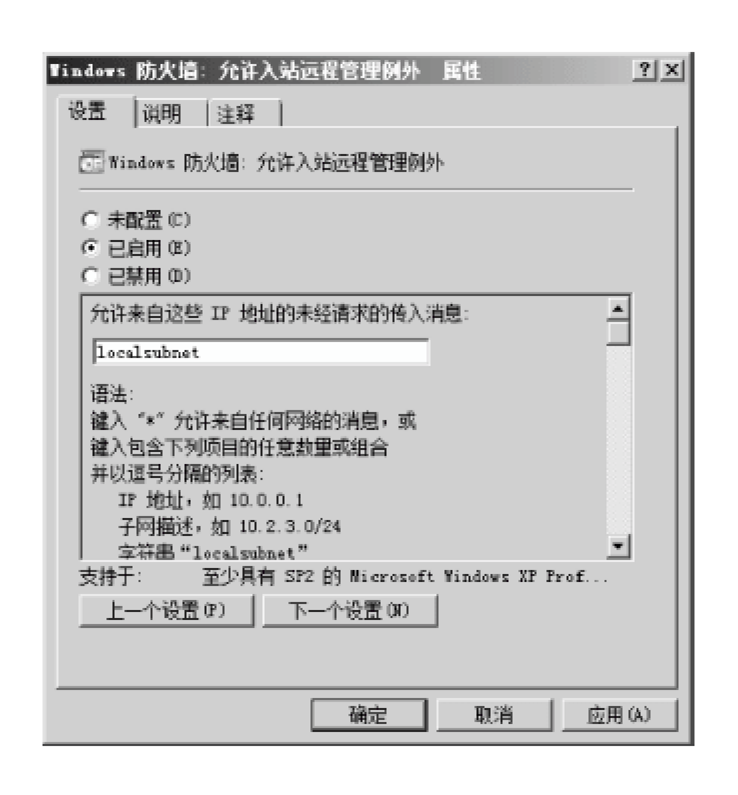
Windows XP 内置了防火墙，对于“单机上网”的计算机来说，这是一个很方便的事情。但对于企业内部网络来说，如果大家互相共享计算机资源，并且对计算机的防火墙设置不是很熟悉，将无法使用文件和共享打印服务。通过修改组策略的方法，修改 Windows XP 的防火墙设置，为终端计算机启用文件和打印共享，也可以为防火墙打开其他的端口。

(1) 在“组策略管理编辑器”窗口中，依次展开“计算机配置”→“管理模板：从本地计算机检索到的策略定义”→“网络”→“网络连接”→“Windows 防火墙”→“域配置文件”目录，将“Windows 防火墙：不允许例外”策略的值修改为“已禁用”状态。

(2) 将“Windows 防火墙：允许入站远程管理例外”修改为“已启用”状态，并且在“允许来自这些 IP 地址的未经请求的传入消息”文本框中输入 localsubnet，如图 11-21 所示。

(3) 将“Windows 防火墙：允许入站文件和打印机共享例外”修改为“已启用”状态，并

在“允许来自下列 IP 地址的未经请求的传入消息”文本框中输入 localsubnet，如图 11-22 所示。





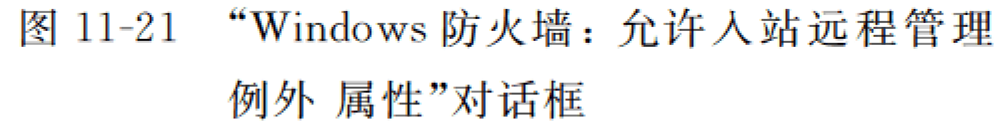


图 11-21 “Windows 防火墙：允许入站远程管理例外 属性”对话框

图 11-22 “Windows 防火墙：允许入站文件和打印机共享例外 属性”对话框

（4）如果想允许其他的服务，如远程桌面，则启用“Windows 防火墙：允许入站远程桌面例外”，并输入允许的地址。

（5）如果想允许其他未列出的服务，则启用“Windows 防火墙：定义入站端口例外”，将这一项修改为“已启用”后，并单击“显示”按钮，在“显示内容”对话框中，单击“添加”按钮，并按照以下格式添加服务即可，如图 11-23 所示。

<Port>:<Transport>:<Scope>:<Status>:<Name>

其中<Port>是十进制的端口号，<Transport>是 TCP 或 UDP，<Scope>是“ * ”作用范围（ * 用于所有网络和 IP 地址或子网），例如，在 Windows XP 的计算机上安装了 Web 服务器，想允许外网的用户使用，则需要输入以下内容。

80:TCP: * :enabled:Http Server

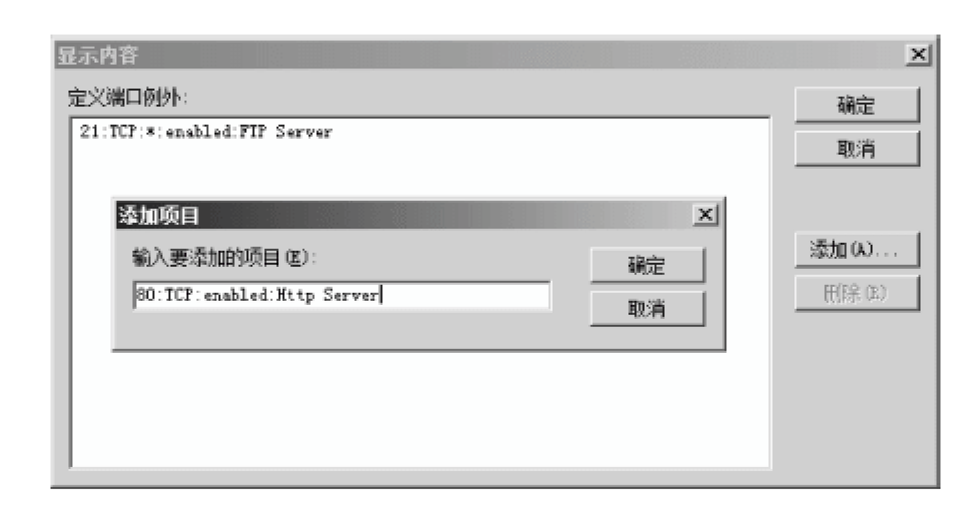


图 11-23 添加其他端口

（6）依次单击“确定”按钮，保存设置并退出。

说明：虽然可以在这一项禁止 Internet 连接防火墙，但如果计算机的本地管理员在域策略生效之后（即禁用 Internet 连接防火墙之后），手动启用了 Internet 连接防火墙，则本地管理员的操作将覆盖组策略的设置（只对当前计算机有效）。

11.4.2 设备限制安全策略

通过在所有客户端计算机上部署硬件设备安装限制安全策略，可以阻止用户随便在计算机上安装任何硬件设备，防止不必要的系统安全问题，例如，通过限制使用 U 盘等可移动存储设备，不仅可以阻止部分病毒的传播，还可以避免重要的信息失窃。组策略中的管理模板策略有两个级别的控制权，第一个级别可以阻止设备驱动的安装，特别是移动存储设备；第二个级别控制对资源的访问。管理员通过限制从可移动存储设备中读取和向其中写入的

数据，就可以保护内部数据安全。

提示：此处以硬件设备的 GUID 为例，禁止安装指定的硬件设备。

(1) 将任意 U 盘插入计算机的 USB 接口，打开“计算机管理”→“设备管理器”窗口，展开“磁盘驱动器”目录，显示图 11-24 所示的窗口。

(2) 右击 U 盘对应的设备名称，选择“属性”命令，在打开的对话框中选择图 11-25 所示的“详细信息”选项卡。在“属性”下拉列表框中选择“设备类 GUID”选项，在“值”列表框中，显示的就是 U 盘类设备对应的 GUID，将此值复制到剪贴板即可。

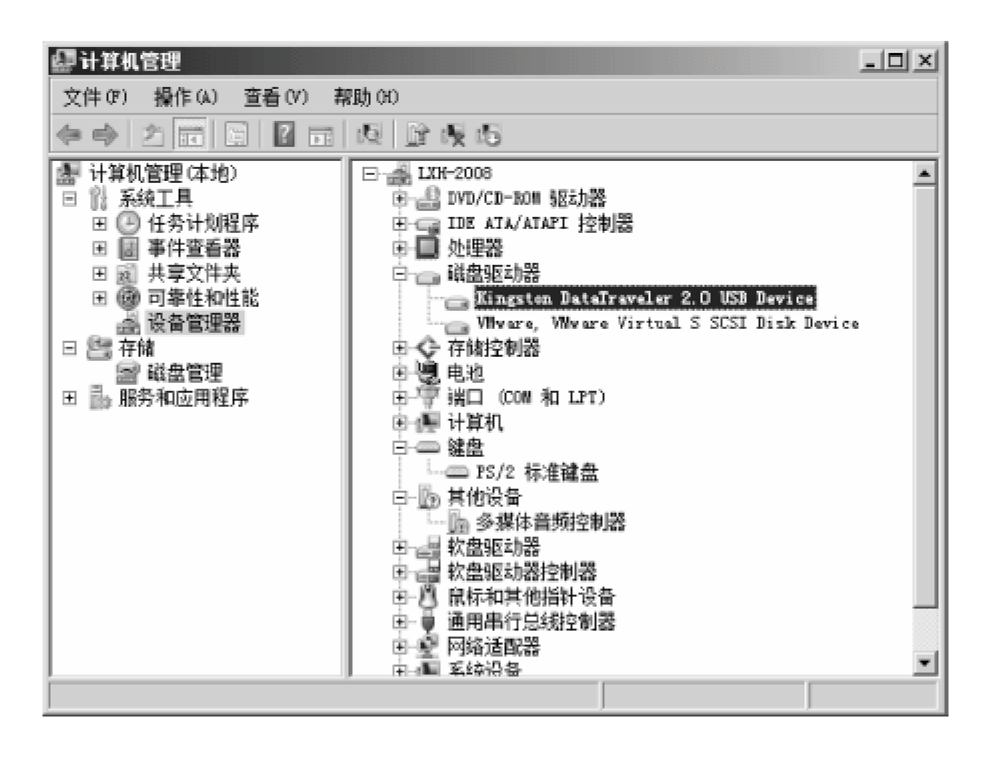


图 11-24　“计算机管理”窗口

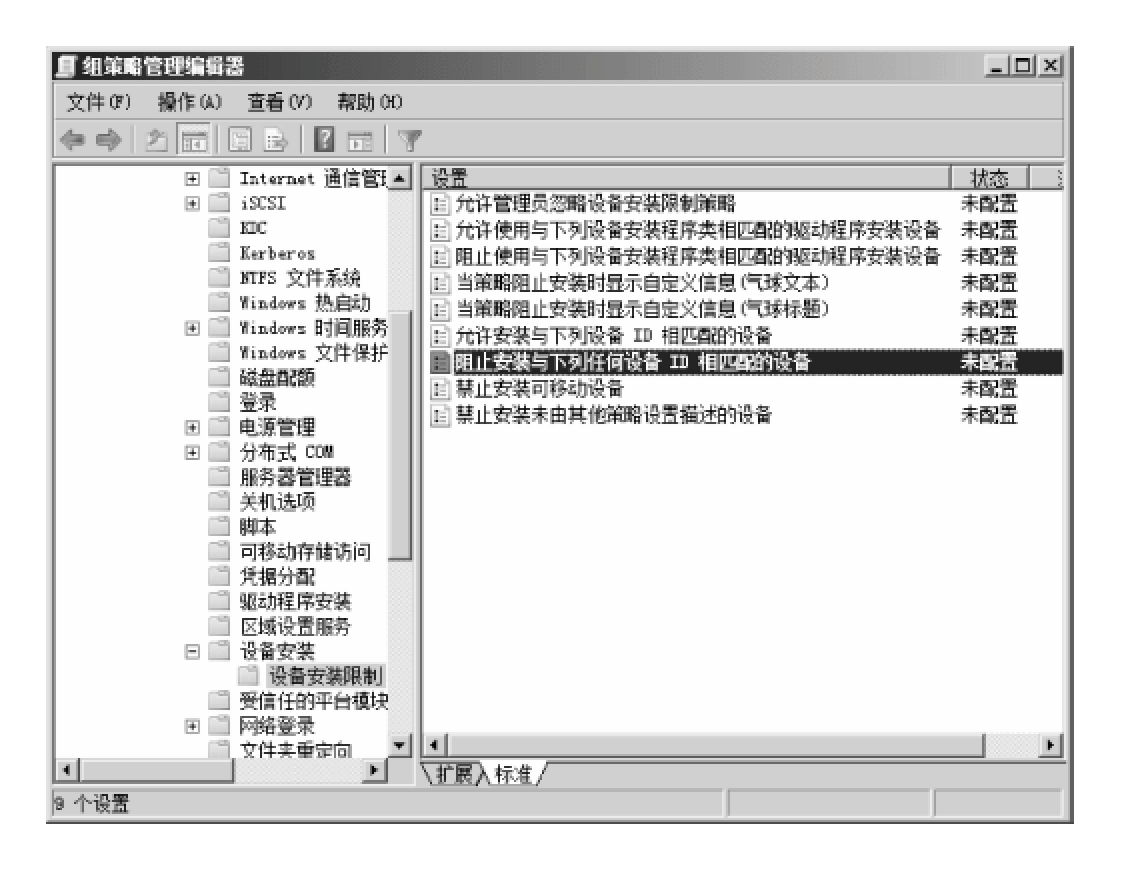


图 11-25　“详细信息”选项卡

(3) 单击“确定”按钮，关闭对话框。

(4) 在“组策略管理编辑器”窗口中，依次展开“计算机配置”→“管理模板”→“系统”→“设备安装”→“设备安装限制”目录，显示图 11-26 所示的窗口。

(5) 双击“阻止安装与下列任何设备 ID 相匹配的设备”策略，显示图 11-27 所示的对话框，选中“已启用”单选按钮。



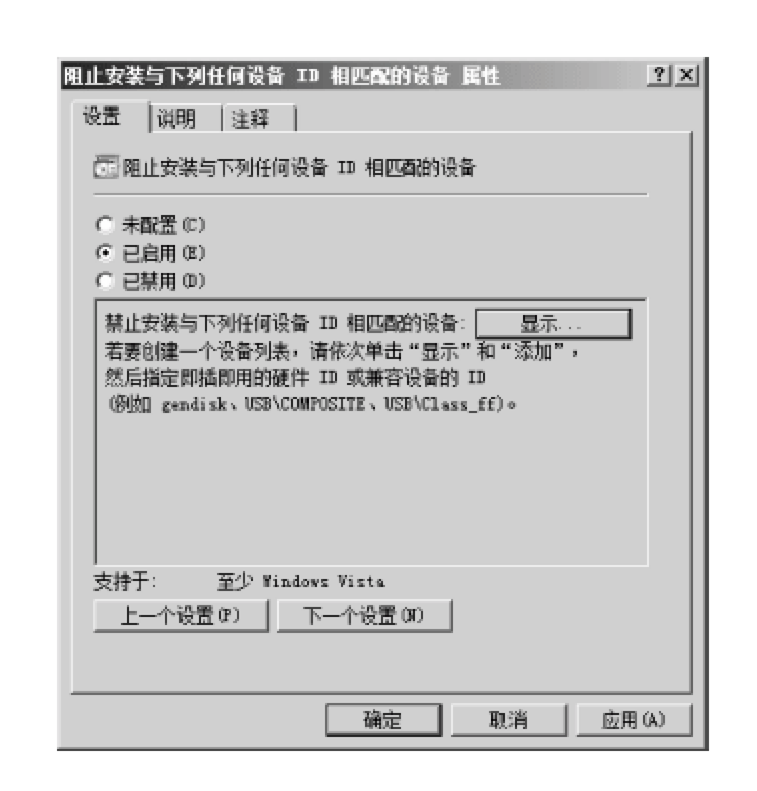


图 11-26　“组策略管理编辑器”窗口

图 11-27　“阻止安装与下列任何设备 ID 相匹配的设备 属性”对话框

(6) 单击“显示”按钮，显示“显示内容”对话框，默认此列表为空白。单击“添加”按钮，显示“添加项目”对话框，将复制到剪贴板的 U 盘类设备 GUID，粘贴到“输入要添加的项目”文本框中即可，如图 11-28 所示。

(7) 连续单击"确定"按钮,保存设置即可。由于以上策略只是阻止使用 U 盘类设备,所以应用此策略后,用户仍可以将 U 盘插入 USB 接口,并且系统会自动为其安装驱动程序,但是在资源管理器中打开时,会发现 U 盘对应的可用磁盘空间为 0,不会显示任何数据,如图 11-29 所示。

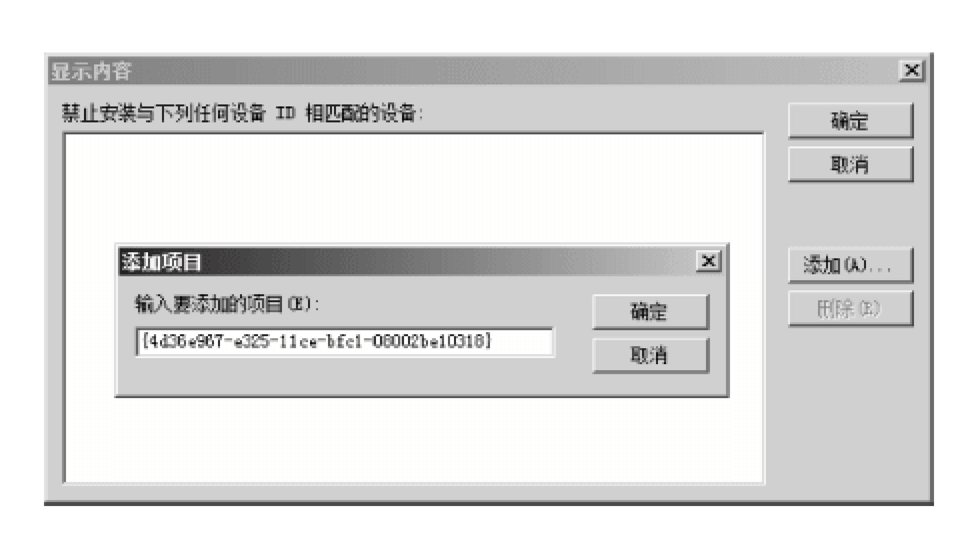


图 11-28 "添加项目"对话框

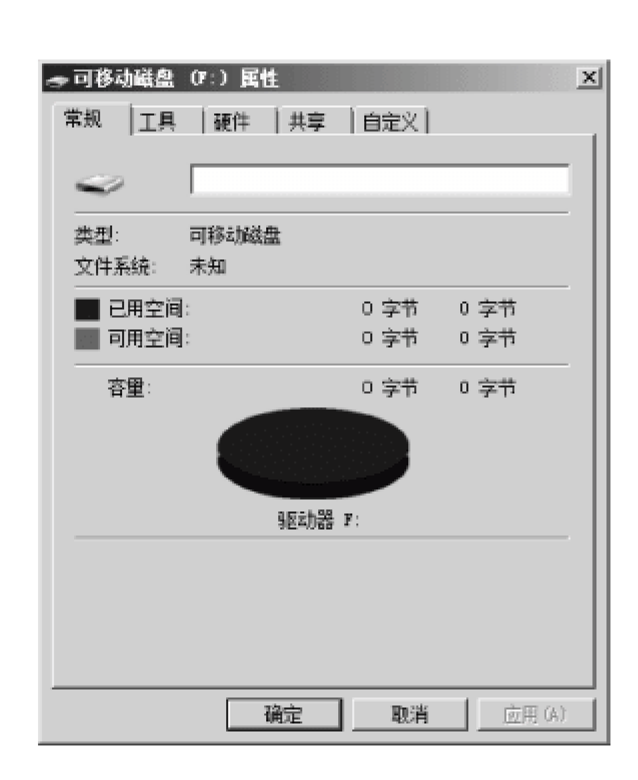


图 11-29 U 盘当前不可用

这些措施并不能从根本上解决核心数据的安全问题,恶意用户仍然可以通过电子邮件发送数据,并且如果是管理员的话,具备工作站或服务器的物理操作权限,则盗取数据更是易如反掌。所以说,最完美的解决方案是确保核心数据的访问权限,而不是仅仅依靠组策略。

注意:如果在应用设备限制策略之前,用户已经将移动设备安装到系统中,则不能阻止用户的正常应用,该策略会在用户取下设备并再次安装移动设备时生效。

11.5 系统和应用程序管理

在网络环境中安装新的软件是每个网络管理员经常遇到而且很烦琐的工作,有没有一种办法简单实用,又不需要管理员不停地楼上楼下安装的方法呢?事实上使用组策略就可以为系统管理员提供这样一种行之有效的办法。

11.5.1 准备工作

在发布软件前,需要进行一些准备工作,以使软件可以正常地发布到客户端计算机。必要的准备工作如下。

(1) 服务器端。在服务器上创建一个共享文件夹 Software,将安装文件使用的 msi 数据包复制到此目录下,并且设置访问权限,至少具备读取的权限。

(2) 客户端。启用客户端计算机上的文件和共享功能。在 Windows Server 2008、Windows Vista/7 系统中,默认状态下网络发现和文件共享功能是关闭的,用户需要手动启用该功能。

(3) 准备要发布的文件。使用组策略发布应用程序对文件格式有严格要求,发布之前必须将应用程序制作成相关格式的安装程序包。

11.5.2　发布 msi 格式的软件

通常情况下，微软所发布的补丁程序都是 msi 格式的文件，这些文件可以直接使用组策略进行发布。

（1）在“组策略管理编辑器”窗口中，在想要发布的计算机所在的组织单位中创建一个组策略。这里仍以 coolpen 组织单位为例进行介绍，创建名为 Core 的组策略，如图 11-30 所示。

图 11-30　“新建 GPO”对话框

（2）单击“确定”按钮，创建新的组策略对象。

（3）右击 Core，在快捷菜单中选择“编辑”命令，显示图 11-31 所示的“组策略管理编辑器”窗口。

（4）依次展开 Core→“用户配置”→“软件设置”→“软件安装”目录，如图 11-31 所示。

（5）右击“软件安装”，在快捷菜单中依次选择“新建”→“数据包”命令，显示图 11-32 所示的“打开”对话框，选择服务器上存储安装文件的共享文件夹。

提示：文件路径必须是网络路径，共享文件位置可以是 DC，也可以是网络上任何一台设备，但是必须具备足够的访问权限。

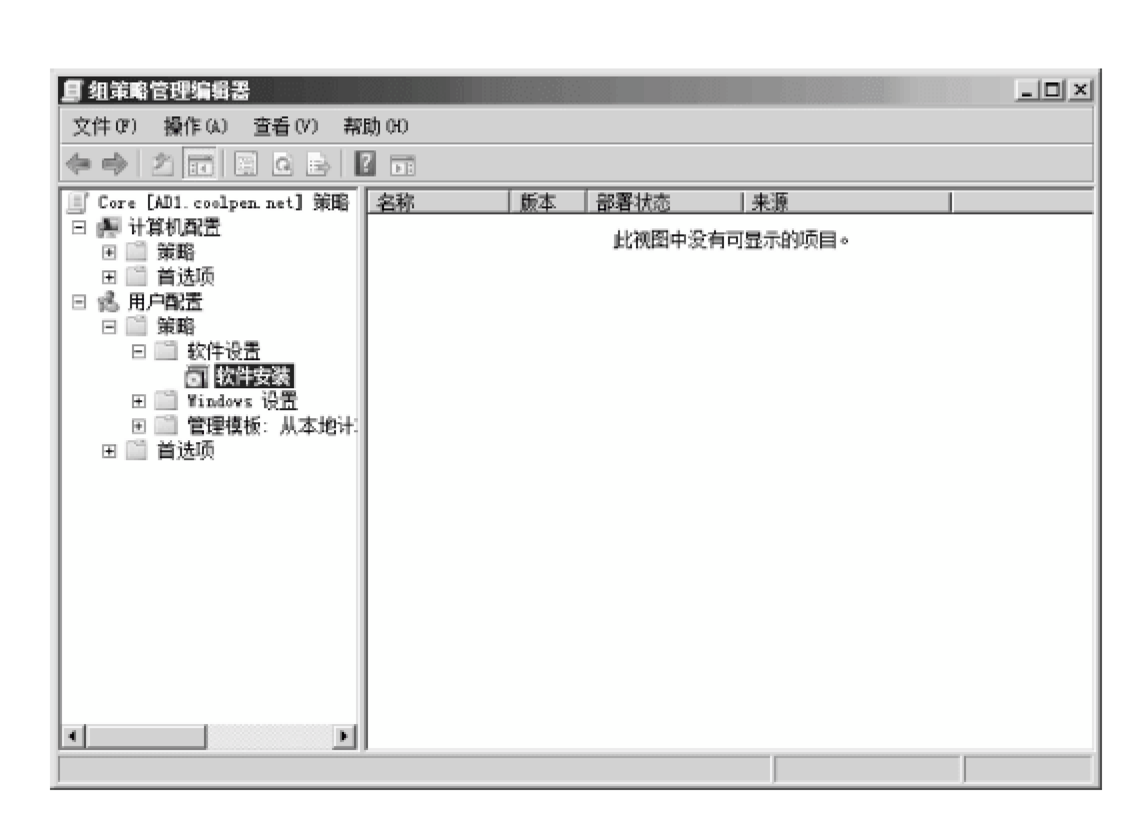


图 11-31　“组策略管理编辑器”窗口

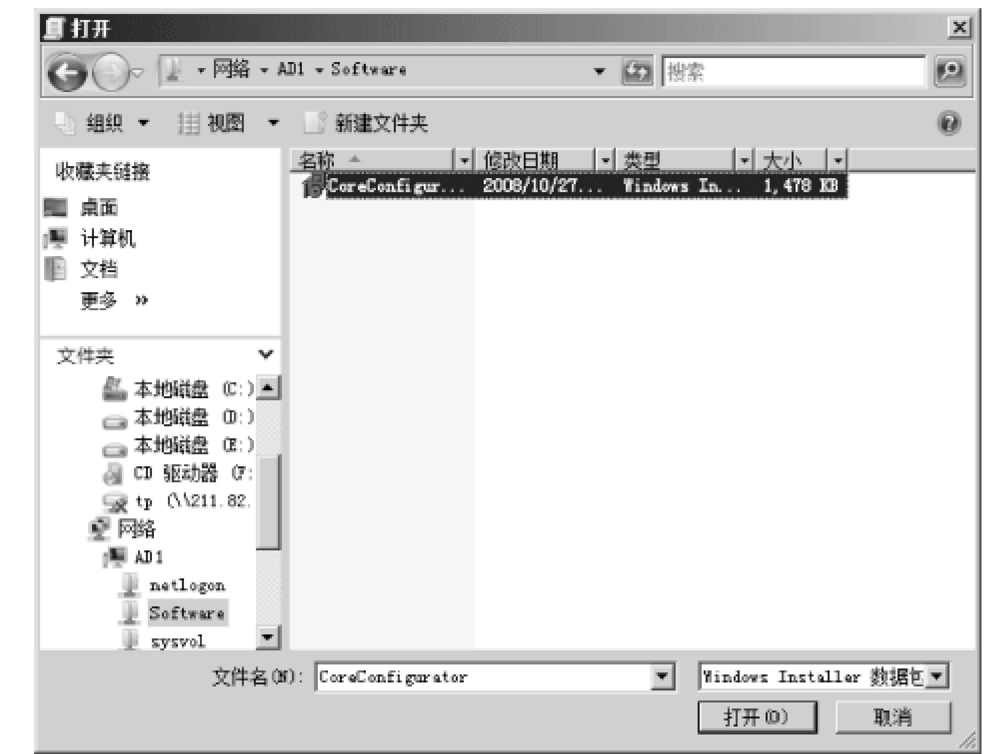


图 11-32　“打开”对话框

（6）单击“打开”按钮，显示图 11-33 所示的“部署软件”对话框。具体各项含义如下。

① 已发布：当某个软件分发给用户以后，组策略生效后，用户在任何一台计算机登录时，所部署的软件将出现在用户计算机的“添加/删除程序”对话框中。此时并没有真正安装或者修改计算机的设置，也没有在“开始”菜单或者桌面上创建快捷方式。只有用户从“添加/删除程序”对话框中或者打开了该软件的关联信息以后，软件会自动下载并安装到用户所在的计算机上。如果用户不需要该软件，可以在“添加/删除程序”对话框中删除该软件。

② 已分配：当软件分配给计算机时，计算机在下一次启动的时候会自动下载并安装软件。在出现系统登录对话框以前，软件已经安装完毕。软件是真正安装到用户的计算机上，不仅仅是通知而已。当软件安装到计算机上后，除非具

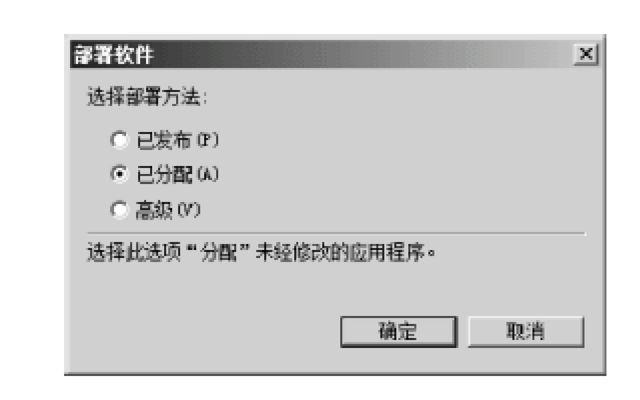


图 11-33　“部署软件”对话框

备管理员权限的用户，其他用户都不能删除该软件，但是用户仍然可以使用“添加/删除程序”对话框来修复或者重新安装受损的程序。

③ 高级：使用该选项配置“已发布”或“已分配”的选项，可用的配置更多。单击“确定”按钮后，会自动打开新建的软件发布策略的属性对话框，此时，根据需要进行配置即可。

(7) 单击“确定”按钮，保存设置。返回图 11-34 所示的“组策略管理编辑器”窗口，即可发现软件发布包已经创建完成。

(8) 右击新建的数据包，在快捷菜单中选择“属性”命令，打开软件发布包的属性对话框。选择“部署”选项卡，如图 11-35 所示。选中“部署选项”区域的“在登录时安装此应用程序”复选框，当用户登录到 Active Directory 时，自动安装应用程序。

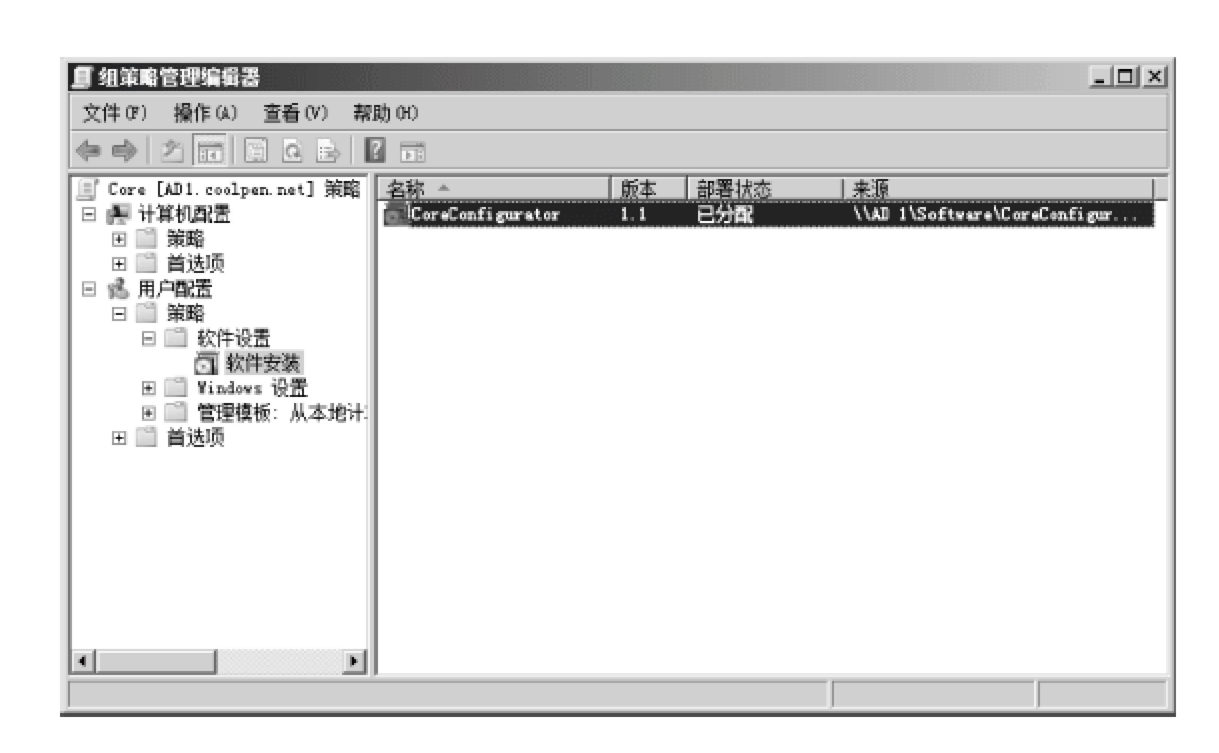


图 11-34 “组策略管理编辑器”窗口



图 11-35 “部署”选项卡

(9) 单击“确定”按钮，完成部署策略的创建。

11.5.3 发布 EXE 安装程序包

使用组策略，可以很容易地发布 MSI 文件，但对于 EXE 文件默认则不能进行发布。另外，Windows 系统的补丁程序许多都是采用 EXE 文件，为了发布 EXE 文件，可以采取两种安装方法，一种是使用 ZAP 文件格式来发布 EXE 文件；一种是将 EXE 文件制作为 msi 文件进行发布。此处以前者为例加以介绍。

1. 创建 ZAP 文件

微软公司提供了使用 ZAP 文件格式来描述补丁安装参数的方式，然后通过群组原则的软件分发功能来部署。ZAP 文件是一个文本文件，它类似于 INI 文件，提供了如何安装应用程序、补丁的相关信息。

创建 acdsee.zap 文件，该文件为文本文件，位于 D:\Software 目录下，如图 11-36 所示。

内容如下。

```
[Application]
Friendlyname="ACDSee"
Setupcommand="acdsee.exe"
DisplayVersion=10.0
Publisher=ACDSee
[ext]
```



图 11-36 安装信息描述文件的内容

exe=

参数说明如下。

(1) Friendlyname：信息提示。

(2) Setupcommand：指定自动化安装程序需要执行的命令。

(3) DisplayVersion：显示补丁的版本信息。

(4) Publisher：补丁程序的发布者。

(5) ext：在此部分添加的扩展名称将成为自动安装文件的关联。

注意：ZAP 文件指向实际的安装文件，以便于运行。系统管理员应该确保安装程序的命令行确实就是指向 ZAP 文件的安装程序的位置。在建立完成 ZAP 文件后不要移动它，移动之后 ZAP 将不能正常工作。最简单的办法是将安装文件与 ZAP 文件复制到相同的目录中。这样，就不需要输入任何路径来指明安装文件的位置。

2. 指定安装目录

将安装程序复制到 D 盘的共享文件夹 Software 中，将创建的 ACDSee.zap 文件复制到当前目录下，使补丁程序安装文件和安装信息描述文件在同一目录下。

注意：设置该共享文件夹的权限和网络用户访问该文件夹的权限，同时设置域用户对该文件夹的访问权限。

3. ZAP 软件部署策略

ZAP 软件部署策略的步骤如下。

(1) 打开“组策略管理”窗口，在想要发布的计算机所在的组织单位中创建一个组策略，如图 11-37 所示。

(2) 单击“确定”按钮，创建新的组策略对象。

(3) 右击 ACDSee 按钮，在快捷菜单中选择“编辑”命令，打开“组策略管理编辑器”窗口。依次展开 Core→“用户配置”→“软件设置”→“软件安装”目录。

(4) 右击“软件安装”选项，在快捷菜单中依次选择“新建”→“数据包”命令，显示图 11-38 所示的“打开”对话框。在“文件名”右侧的下拉列表框中选择“ZAW 早期版本应用程序数据包(*.zap)”选项，然后选择服务器上存储安装文件的共享文件夹。需要注意的是，此处也必须使用网络路径。

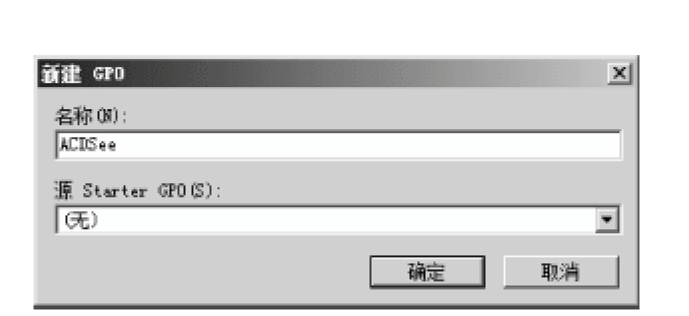


图 11-37　新建组策略



图 11-38　“打开”对话框

(5) 单击"打开"按钮,显示图 11-39 所示的"部署软件"对话框。计算机配置与用户配置的软件发布规则稍有不同,只能选中"已发布"单选按钮。

(6) 单击"确定"按钮,保存设置。返回图 11-40 所示的"组策略管理编辑器"窗口,即可发现软件发布包已经创建完成。

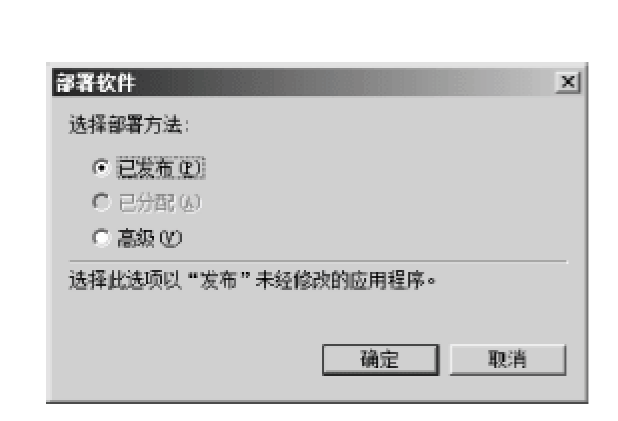


图 11-39 "部署软件"对话框



图 11-40 "组策略编辑器"窗口

注意:使用 zap 文件的方式安装系统补丁时,安装的对象只能是使用者,并且使用者通过 zap 的方式安装补丁的时候,必须具备管理员的权限,不具备管理员权限的用户登录安装补丁时,会因为权限不足而导致安装补丁失败。

习题

使用组策略可以对客户端进行哪些配置?

实验:为客户端分发 EXE 软件安装包

实验目的:

掌握使用组策略分发软件的技术。

实验内容:

创建 EXE 安装程序的 ZAP 文件,并使用组策略分发在网络中的客户端上。

实验步骤:

(1) 创建 ZAP 文件。

(2) 将安装文件复制到共享文件夹中,并指定该安装目录。

(3) 创建 ZAP 软件部署策略。

第 12 章 chapter 12

系统故障诊断与排除

当按计算机的电源键时，服务器就开始了一系列复杂的启动过程。但由于种种原因，系统并不是每次都可以正常地启动，因此，需要在系统无法正常启动时，快速地排除故障，并使系统正常启动。

12.1 系统故障诊断与排除规划

通常情况下，系统故障的发生是不可预料的，并且也是不可避免的。如何根据网络需要施行必要的保护措施，从而将由系统故障而造成的损失降到最低，这是每个管理员必须学习的知识。

12.1.1 项目背景

鉴于服务器在网络中的重要作用，保证服务器的正常运行就显得尤其重要。无论采用多全面的保护措施，都不能保证服务器一直保持正常工作，难免会发生不同的故障。另外，除服务器自身发生故障外，人为所造成的故障也是不容忽视的。因此，做好必要的备份也是减少由发生故障而造成损失的必要工作。

12.1.2 项目需求

在该项目中，最重要的服务器是域控制器，在域控制器上保存着企业中的所有用户账户信息，如果这些内容因为服务器故障而丢失，其损失是无法估量的。因此，在日常服务器的管理中，应对服务器进行相关的备份操作，例如设置备份计划，可以让服务器定时对所设置的内容进行备份，从而使在故障发生时，所还原的数据是最新的。

12.1.3 解决方案

对于服务器的备份与恢复，通常情况下，可以通过如下两种方法实现。

（1）使用服务器自身的备份机制，在发生故障时使用最近一次正确的配置。

（2）安装备份角色，通过进行备份操作，在服务器发生故障时使用备份进行还原，达到恢复服务器的目的。

12.2 选择“最近一次的正确配置”启用系统

每次系统正常启动，并且用户正常登录后，系统就会将当前的系统配置进行一次保存，这里所保存的当前系统配置，就是所谓的“最近一次的正确配置”。如果因为用户更改了系统配置，造成系统无法启动的话，则可以使用所保存的“最近一次的正确配置”来修复系统。

(1) 按计算机电源开关，并迅速按 F8 键，显示图 12-1 所示的“高级启动选项”菜单窗口。

(2) 使用方向键选择“最近一次的正确配置(高级)”菜单项，然后按 Enter 键，系统即可从“最近一次的正确配置”启动系统。



图 12-1 “高级启动选项”菜单窗口

知识链接：“最近一次的正确配置”使用情况

在下列情况下，可以使用“最近一次的正确配置”来启动 Windows Server 2003 系统。

(1) 当为计算机安装了新的驱动程序后，而造成 Windows Server 2003 停止响应或无法启动。

(2) 默认情况下，系统中有些接口或服务是不能禁用的，禁用这些接口或服务可能会造成系统无法启动。

并不是所有的场合都适用“最近一次的正确配置”，也有一些场合是不适用的，具体包括如下内容。

(1) 系统故障并不是由系统配置引起的，例如重新安装设备驱动程序等。

(2) 因为硬件故障或系统文件损坏而造成的系统无法启动。

(3) 当发生故障后，用户又成功登录。这主要是因为发生故障后的成功登录会重新生成一次“最近一次的正确配置”，而将先前的“最近一次的正确配置”覆盖掉。

12.3 服务器操作系统的备份与还原

对于服务器而言，仅使用“最近一次的正确配置”是远远不够的，这是因为通常在服务器中会保存有大量的重要数据，例如用户账户信息、系统设置等。因此，为了保证在服务器操作系统发生故障时，可以将损失降到最低，建议使用系统自带的备份功能进行备份，在发生严重故障时使用该功能进行还原。Windows Server Backup 支持图形模式和命令行模式，对于域控制器的备份而言，既可以支持域控制器完整备份，又同时支持组件备份。

12.3.1 安装“备份”功能

Windows Server 2008 中没有提供类似于 Windows Server 2003 或 Windows XP 的“备

份和还原向导”，取而代之的是 Windows Server Backup 备份工具，该工具默认是不被安装的，需要在“服务器管理器”中手动添加。

（1）在“服务器管理器”窗口中，展开“功能”目录，在窗口右侧单击“添加功能”链接，显示图 12-2 所示的“选择功能”对话框。在“功能”列表框中，选中“Windows Server Backup 功能”复选框。默认情况下，只选中 Windows Server Backup 复选框，根据需要还可以安装命令行工具。



图 12-2 “选择功能”对话框

当选中“命令行工具”复选框时，显示图 12-3 所示的“添加功能向导”对话框。提示需要安装 Windows PowerShell 工具，单击“添加必需的功能”按钮，同意安装该功能即可。

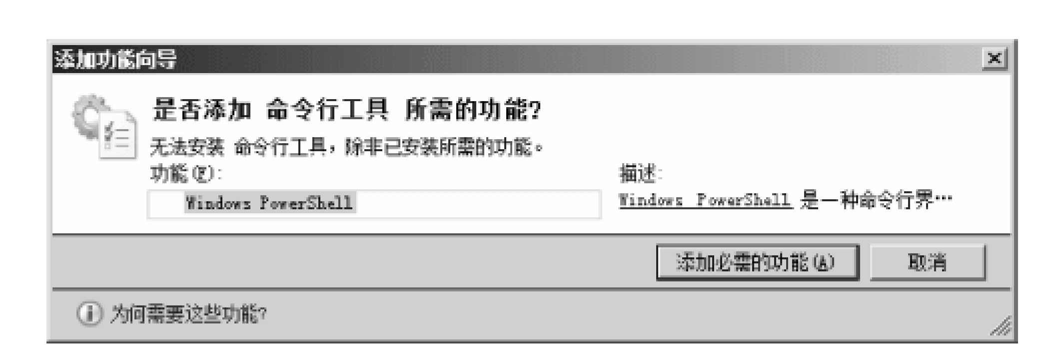


图 12-3 “添加功能向导”对话框

（2）单击“下一步”按钮，显示“确认安装选择”对话框，显示了前面选择的要安装的功能，如果安装完成之后需要重新登录系统或重新启动服务器，这里也会出现提示信息。

（3）单击“安装”按钮，即可开始安装。安装完成后显示图 12-4 所示的“安装结果”对话框，如果全部安装成功则不会出现报错信息，如果未能安装成功则会提示失败的原因及修复方法。

（4）单击“关闭”按钮，关闭安装向导即可。

12.3.2 设置备份有效时间

当活动目录中的一个对象被删除时，该对象并不会被彻底删除，而会成为一个被标记为“墓碑记录”的记录。在 Windows Server 2008 中，默认的“墓碑记录”生存周期为 180 天，180 天之后被标记为“墓碑记录”的记录才会被永久删除。在默认状态下，不能从比墓碑默认的生存记录时间更久的系统状态备份数据中恢复 Active Directory 数据库。



图 12-4　安装结果

通常情况下，为了实际需要，用户可以修改该墓碑的生存时间，具体操作步骤如下。

（1）依次选择“开始”→“管理工具”→ADSI Edit 命令，显示 ADSI Edit 窗口。右击左侧窗口的 ADSI Edit 选项并在快捷菜单中选择“连接到”命令，显示图 12-5 所示的“连接设置”对话框。在“选择一个已知命名上下文”下拉列表框中选择“配置”选项。

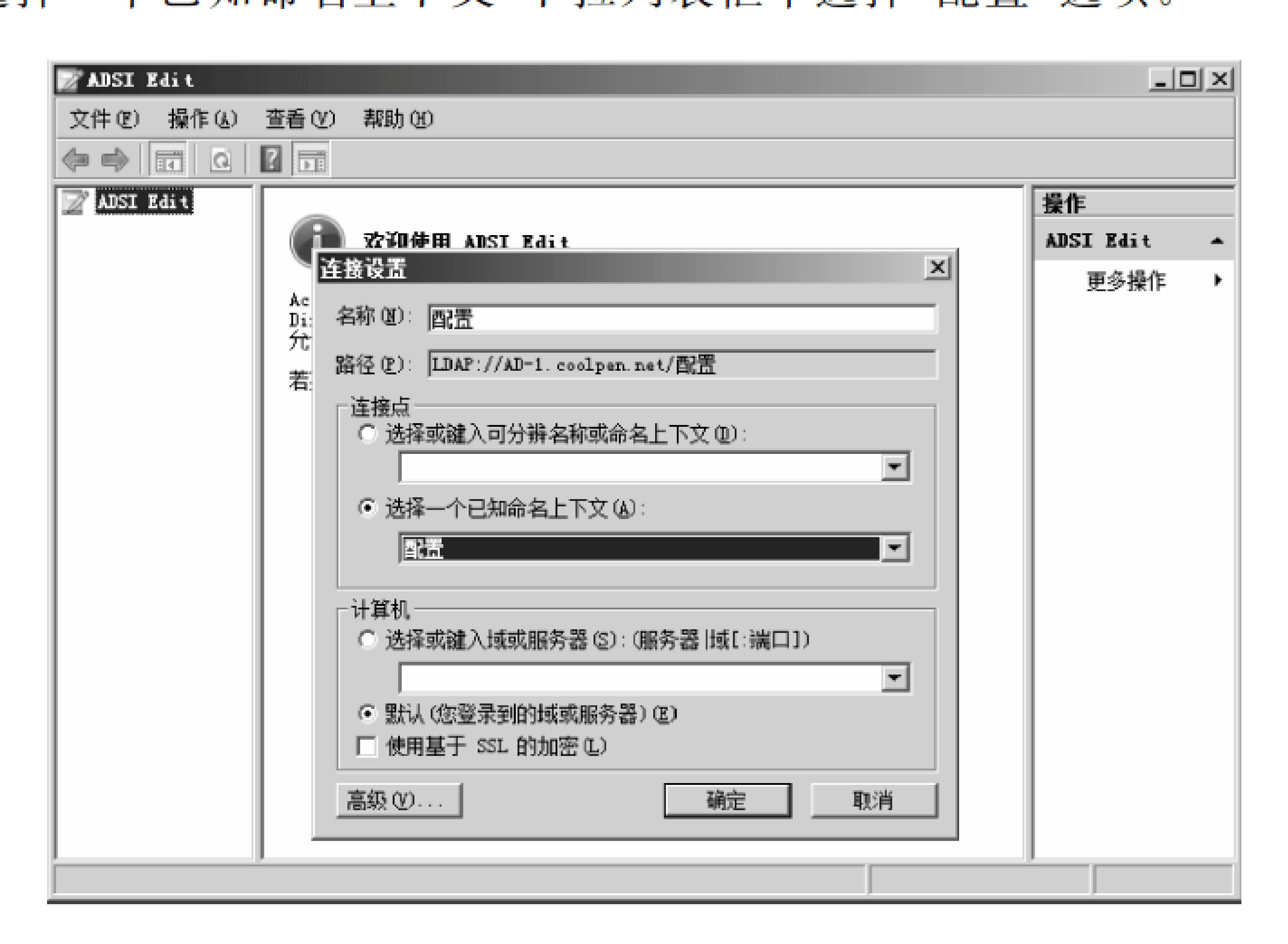


图 12-5　“连接设置”对话框

（2）单击“确定”按钮，关闭“连接设置”对话框，返回到 ADSI Edit 窗口。

（3）在左侧栏中，依次展开“配置[AD-1.coolpen.net]”→CN＝Configuration，DC＝coolpen，DC＝net→CN＝Services→CN＝Windows NT→CN＝Directory Service 目录，如图 12-6 所示。

（4）右击 CN＝Directory Service 选项并在快捷菜单中选择“属性”命令，显示图 12-7 所示的“CN＝Directory Service 属性”对话框。在“属性”列表中，选择 tombstoneLifetime 选项。



图 12-6　配置内容



图 12-7　“CN＝Directory Service 属性”对话框

（5）单击“编辑”按钮，显示图 12-8 所示的“整数属性编辑器”对话框。在“值”文本框中，输入新的墓碑生存时间即可，例如 360。

（6）依次单击“确定”按钮，保存设置，即可完成墓碑记录时间的修改。



图 12-8　“整数属性编辑器”对话框

12.3.3　完全备份

完全备份是指备份当前服务器的所有数据，即所有逻辑磁盘上的文件，此时可能要花费较多的时间，但备份数据全面，可操作性强。备份数据可以选择保存在本地 DVD 驱动器的可写入磁盘上，也可以选择网络上的共享目录作为目标路径。

（1）依次选择“开始”→“管理工具”→Windows Server Back 命令，打开图 12-9 所示的 Windows Server Backup 窗口。也可以在“运行”对话框中，输入 wbadmin.msc 启动备份工具。



图 12-9　Windows Server Backup 窗口

(2) 在右侧“操作”窗格中，单击“一次性备份”链接，启动备份向导，如图 12-10 所示。由于没有配制备份计划，所以只能选中“不同选项”单选按钮。

(3) 单击“下一步”按钮，显示图 12-11 所示的“选择备份配置”对话框。选中“整个服务器(推荐)”单选按钮，即备份当前服务器的所有数据、应用程序和系统状态。

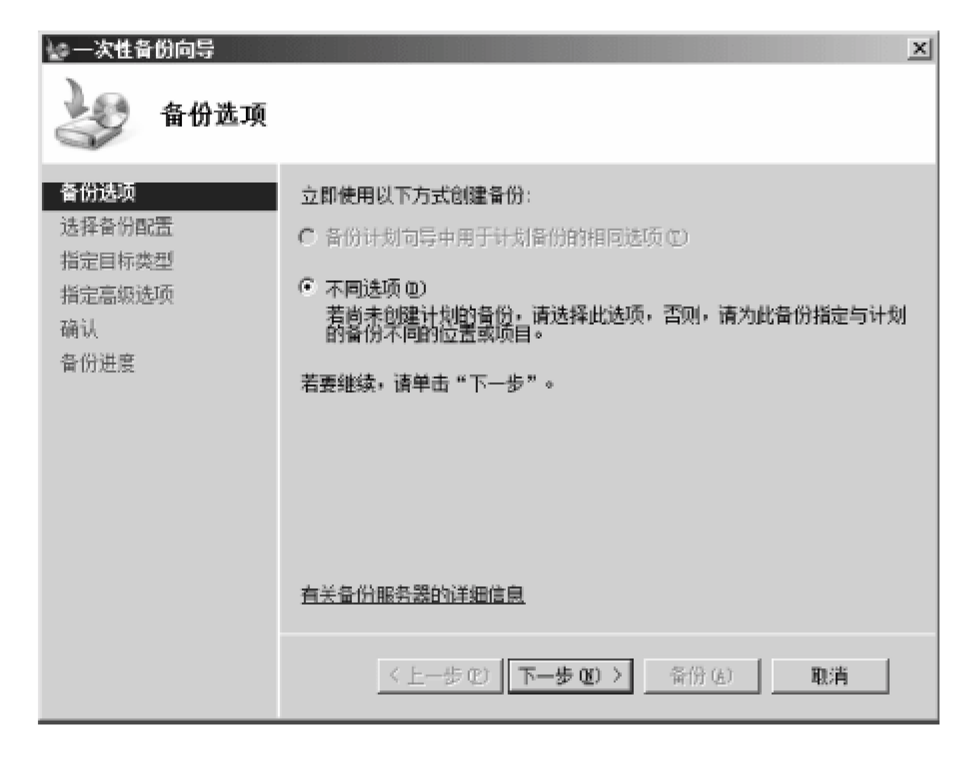



图 12-10 “备份选项”对话框



图 12-11 “选择备份配置”对话框

注意：在此之前，如果已经创建了该服务器的备份，则继续执行备份将可能导致原来的备份被覆盖。此时，会显示图 12-12 所示的提示框，如果单击“否”按钮，将退出该向导，单击“是”按钮，可继续备份操作，同时也会覆盖原备份文件。

(4) 单击“下一步”按钮，显示图 12-13 所示的“指定目标类型”对话框。选中“本地驱动器”单选按钮，可以将备份保存至本地逻辑驱动器或 DVD 驱动器；选中“远程共享文件夹”单选按钮，可以将备份保存至局域网中指定的共享文件夹中。这里选中“远程共享文件夹”单选按钮。

提示：建议将备份保存至 DVD 驱动器或远程共享文件夹中，这样安全程度相对较高。如果保存至本地磁盘，则将自动从备份目标中剔除作为保存目录的磁盘分区，并且服务器出现磁盘故障时，备份数据也将丢失。

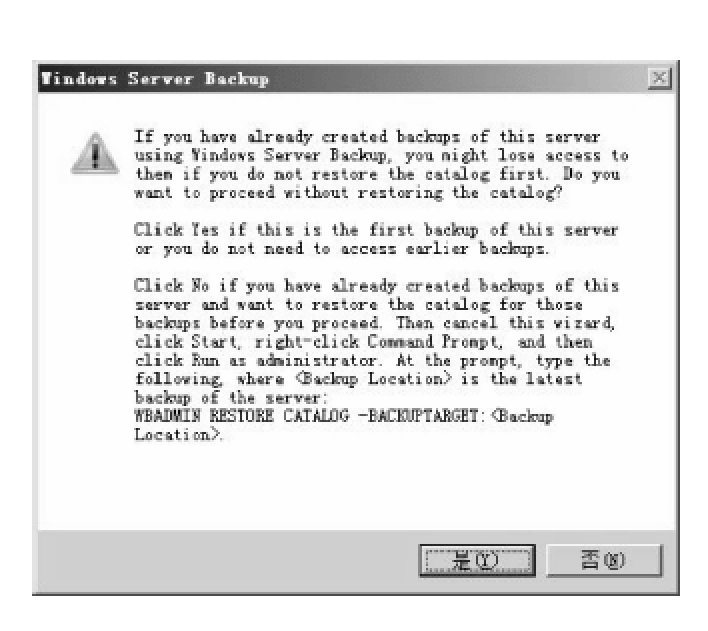


图 12-12 提示信息



图 12-13 “指定目标类型”对话框

(5) 单击“下一步”按钮，显示图 12-14 所示的“指定远程文件夹”对话框。在“请输入远程共享文件夹的路径”文本框中，输入目标路径。在“访问控制”选项区域中，选中“不继承”单选按钮，则可以为特定的用户账户赋予访问此备份的权限，如果选中“继承”单选按钮，则

任何用户账户都可以访问备份文件。

(6) 单击“下一步”按钮，显示图 12-15 所示的“提供用于备份的用户凭据”对话框，分别在“用户名”和“密码”文本框中，输入具体共享文件夹访问权限的用户名和密码。需要注意的是，该用户必须是远程计算机中已经赋予足够权限的用户账户，否则备份将无法顺利进行。





图 12-14　“指定远程文件夹”对话框



图 12-15　“提供用于备份的用户凭据”对话框

(7) 单击“确定”按钮，显示图 12-16 所示的“指定高级选项”对话框。如果使用第三方的备份软件，建议选中“VSS 副本备份(推荐)”单选按钮；如果使用 Windows Server 2008 提供的备份程序，建议选中“VSS 完全备份”单选按钮。

(8) 单击“下一步”按钮，显示图 12-17 所示的“确认”对话框。显示已经设置的“备份项目”、“备份目标”以及“高级选项”等，单击“上一步”按钮可返回重新设置。

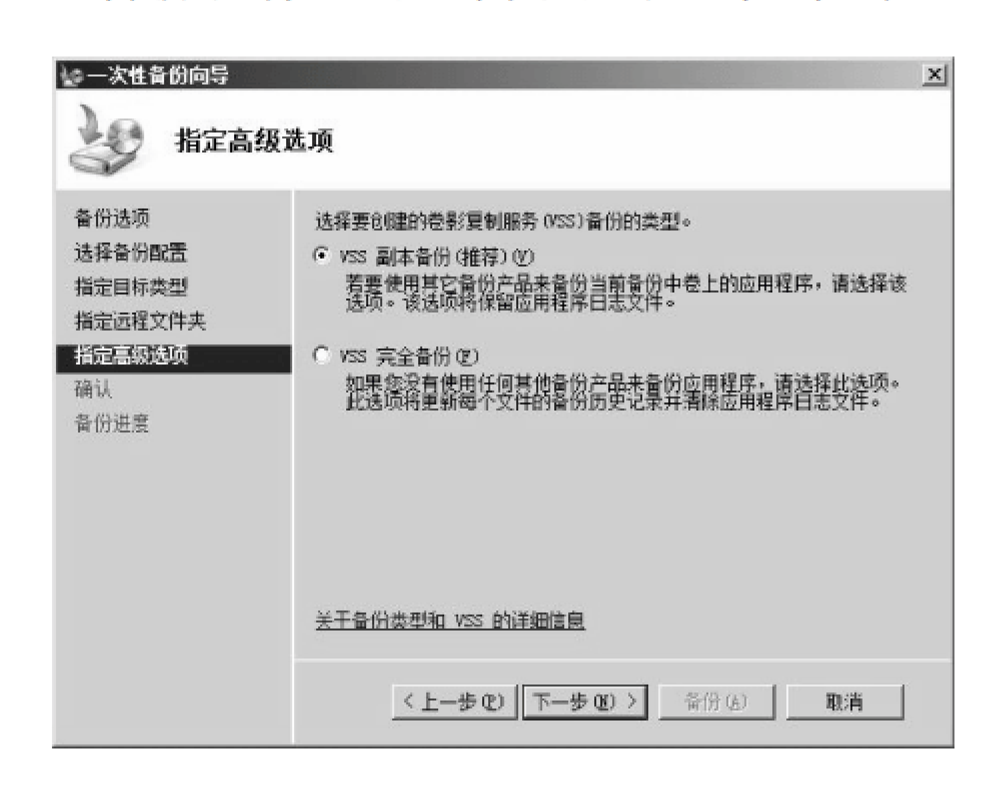


图 12-16　“指定高级选项”对话框



图 12-17　“确认”对话框

(9) 单击“备份”按钮，即可开始备份，如图 12-18 所示。如果需要备份的文件较多，则可能需要较长的时间。备份至网络存储器时更应注意确保网络连接的稳定。

提示：备份过程中，可单击“关闭”按钮关闭当前对话框，备份向导将在后台继续运行。

12.3.4　自定义备份

自定义备份允许用户对要备份的分区进行选择，例如只备份系统分区(网络服务关键数据所在分区)，此时备份则可以保存在其他逻辑分区或磁盘，可以节约备份时间开销。在“选择备份配置”对话框中，选中“自定义”单选按钮，并单击“下一步”按钮，打开图 12-19 所示的

“选择备份项目”对话框。在“希望备份哪些卷”列表中，选择想要备份的分区即可。需要注意的是，如果不想备份系统分区，则应取消选中“启用系统恢复”复选框。接下来的其他操作与“完全备份”完全相同，此处不再赘述。

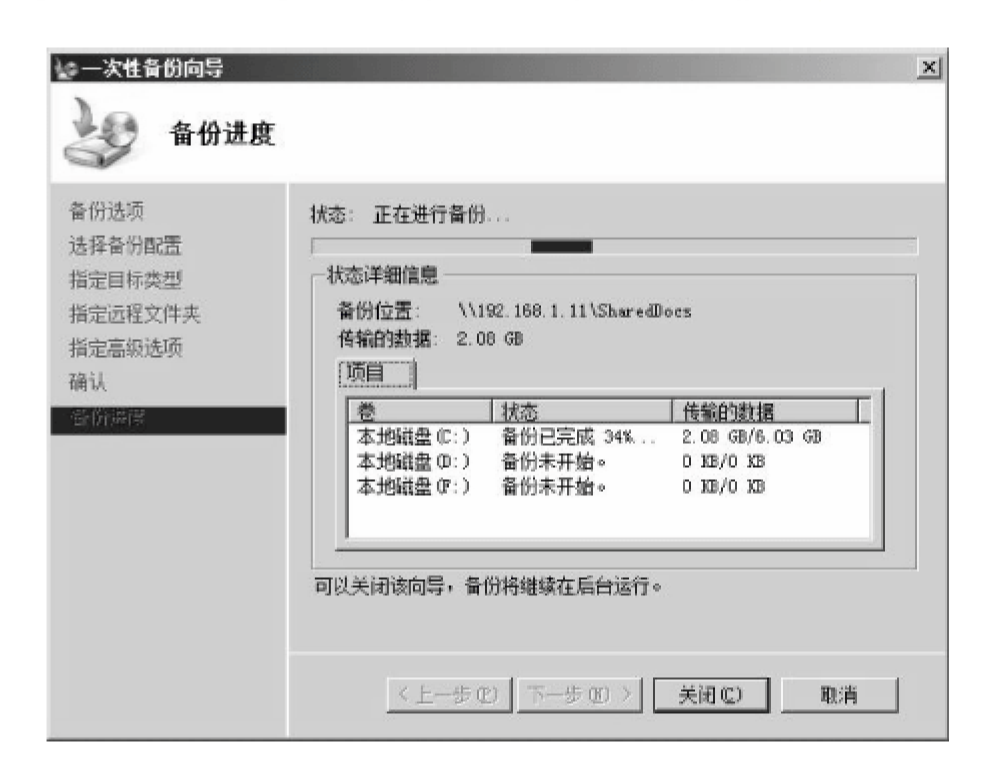


图 12-18 备份进度

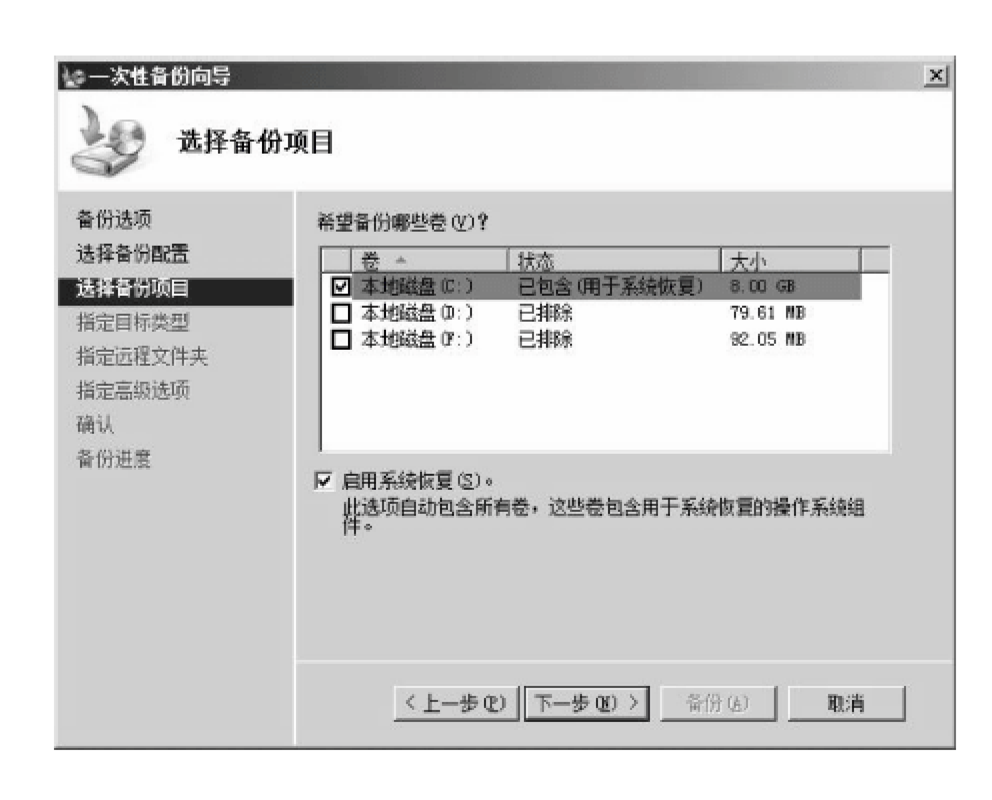


图 12-19 “选择备份项目”对话框

12.3.5 恢复

通过使用恢复功能，可以快速解决由于操作不当或系统故障而导致的服务器无法正常工作的问题。恢复操作同样需要借助 Windows Server Backup 工具完成，具体操作步骤如下。

(1) 在 Windows Server Backup 主窗口中，单击“恢复”链接，打开“入门”对话框。提示选择要从哪个备份恢复服务器数据，既可以使用本地计算机中存储的备份，也可以使用远程计算机共享的该服务器备份，这里选中“此服务器”单选按钮。如果欲从另一台服务器恢复数据，可选中“另一个服务器”单选按钮。

(2) 单击“下一步”按钮，显示图 12-20 所示的“选择备份日期”对话框。用户可以在日期列表中选择备份的日期，如果同一天中保存了多个备份，可以继续在时间下拉列表框中选择不同的时间。



图 12-20 “选择备份日期”对话框

（3）单击“下一步”按钮，显示图 12-21 所示的“选择恢复类型”对话框。选中“文件和文件夹”单选按钮，可根据自己的需要选择备份中需要恢复的文件或文件夹中的数据，操作的前提是备份中包括文件和文件夹，应用程序恢复也是如此；选中“卷”单选按钮，则将恢复指定的磁盘分区。这里选中“卷”单选按钮。

（4）单击“下一步”按钮，显示图 12-22 所示的“选择卷”对话框。选中备份中需要恢复的卷，然后再在“目标卷”下拉列表框中选择需要恢复到的卷。

提示：执行卷恢复后，目标卷上的数据将全部丢失。



图 12-21　“选择恢复类型”对话框



图 12-22　“选择卷”对话框

（5）单击“下一步”按钮，提示恢复卷后将出现的结果，单击“是”按钮继续即可，显示图 12-23 所示的“确认”对话框。如果前面有漏选的需要恢复的项目，则可以单击“上一步”按钮返回修改。

（6）单击“恢复”按钮，即可开始恢复，如图 12-24 所示。根据恢复数据量的大小所需的时间会有所不同，如果源数据位于远程计算机上，则恢复时间还取决于网络传输速率的限制。



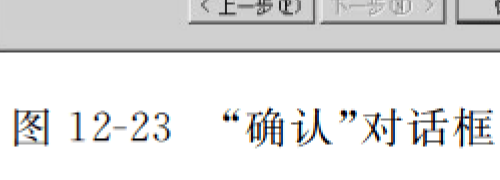


图 12-23　“确认”对话框



图 12-24　“恢复进度”对话框

（7）恢复完成后，单击“关闭”按钮，退出向导即可。

12.3.6　定制备份计划

除手动备份服务器之外，还可以通过定制备份计划实现自动备份。

(1) 在 Windows Server Backup 主窗口中，单击“备份计划”链接，即可启动“备份计划向导”。在“入门”对话框中，直接单击“下一步”按钮，显示图 12-25 所示的“选择备份配置”对话框，系统默认将备份整个服务器上的所有数据，选中“自定义”单选按钮。

(2) 单击“下一步”按钮，显示图 12-26 所示的“选择备份项目”对话框，取消列表中不需要备份的分区即可。需要注意的是，系统分区是不可取消的。

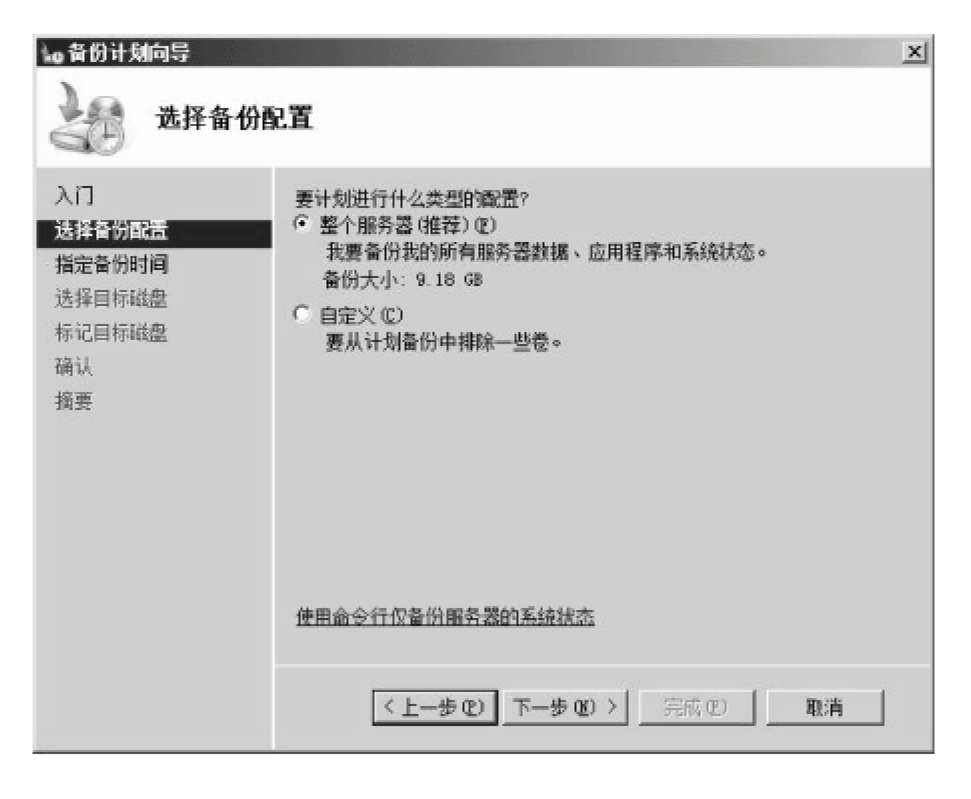
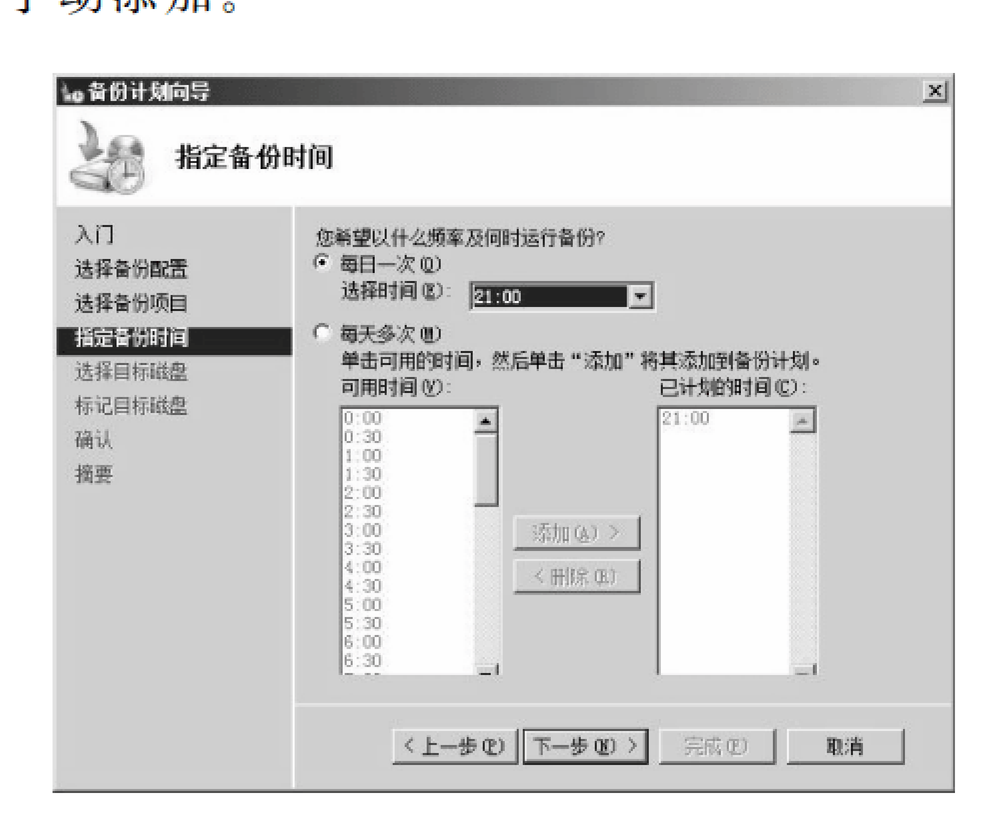


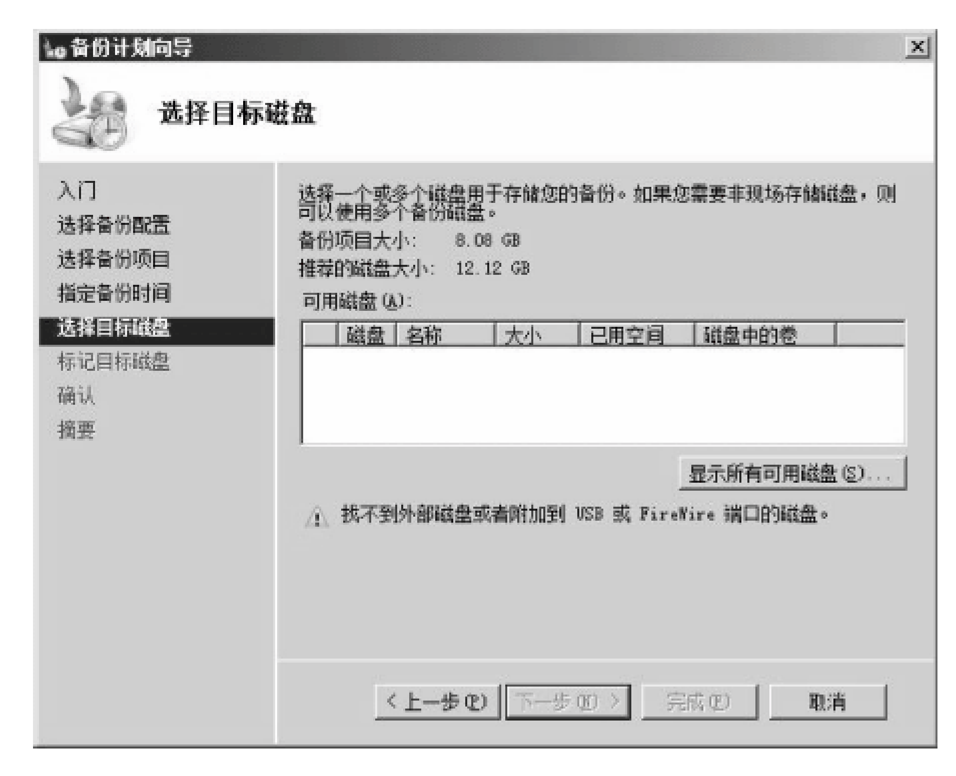
图 12-25 “选择备份配置”对话框

图 12-26 “选择备份项目”对话框

(3) 单击“下一步”按钮，显示图 12-27 所示的“指定备份时间”对话框。选中“每日一次”单选按钮，并在“选择时间”下拉列表框中，选择合适的时间，服务器即可每天自动备份；选中“每天多次”单选按钮，并在“可用时间”列表中，选择指定的时间添加至“已计划的时间”列表中，服务器可每天进行多次自动备份。

(4) 单击“下一步”按钮，显示图 12-28 所示的“选择目标磁盘”对话框。管理员可以选择一个或多个目标磁盘用于存储备份文件，默认情况下，“可用磁盘”列表是空白的，需要用户手动添加。





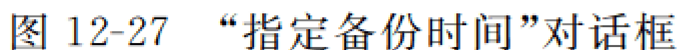

图 12-27 “指定备份时间”对话框

图 12-28 “选择目标磁盘”对话框

(5) 单击“显示所有可用磁盘”按钮，服务器通常会同时挂接多块硬盘，分别用于存储系统、数据、备份等文件，默认在“所有磁盘”列表中会显示所有可以使用的磁盘，即系统所在磁盘之外的其他磁盘。选择用于存储备份的磁盘即可。

(6) 单击“确定”按钮，显示图 12-29 所示的对话框。提示被选磁盘将被重新格式化，磁

盘上的所有数据都将丢失。并且被选择存储备份的磁盘不可再用于存储其他数据，在Windows 资源管理器中也不会显示该磁盘。

(7) 单击“是”按钮，显示图 12-30 所示的“标记目标磁盘”对话框。被选磁盘将自动显示在磁盘列表中，并被标记了标签信息，通常包括服务器名称、备份日期时间等。为了便于区分，建议将该标签信息以便签的方式粘贴在磁盘上面。

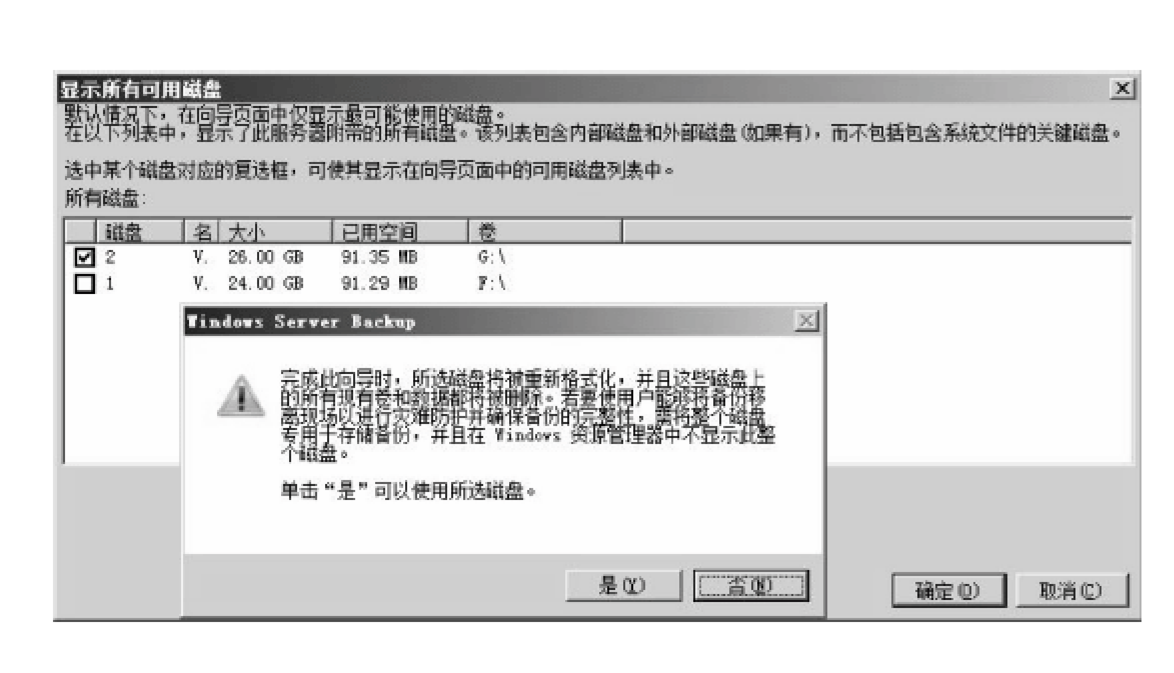



图 12-29　Windows Server Backup 对话框

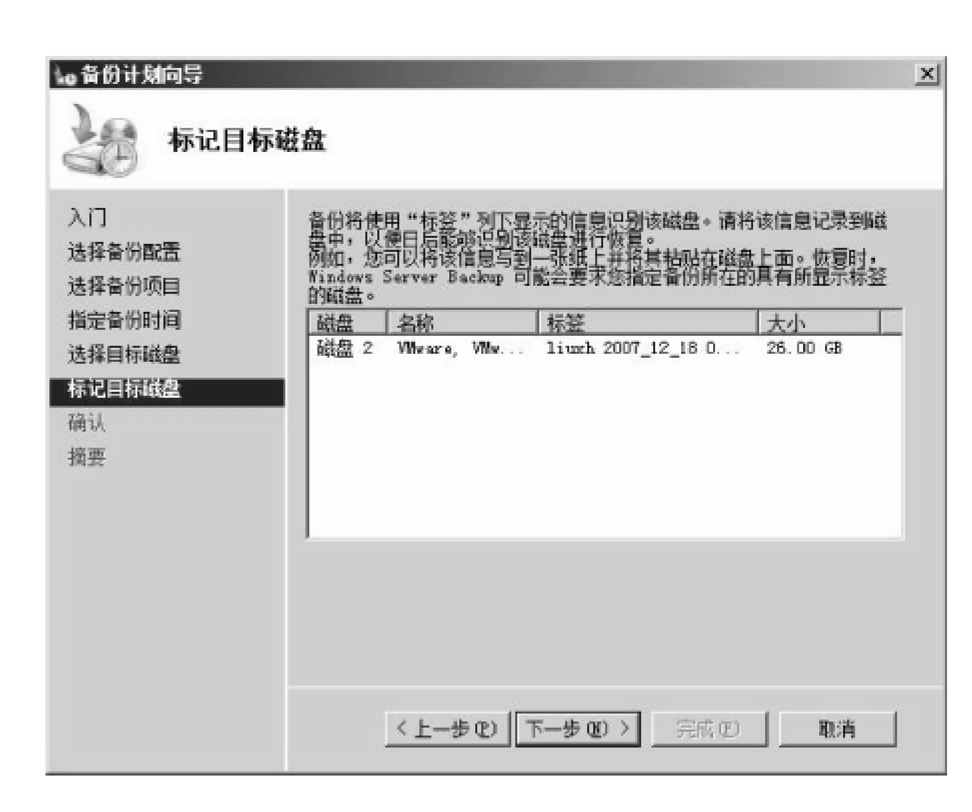


图 12-30　“标记目标磁盘”对话框

(8) 单击“下一步”按钮，显示图 12-31 所示的“确认”对话框，仔细审查备份计划中的所有项目，如需修改可单击“上一步”按钮返回。

(9) 单击“完成”按钮，显示图 12-32 所示的对话框，继续单击“格式化磁盘”按钮即可格式化所选磁盘并完成备份计划。



图 12-31　“确认”对话框



图 12-32　格式化磁盘

(10) 最后，单击“关闭”按钮，退出向导即可。

12.3.7　文件恢复

Windows Server Backup 功能可以恢复备份中的文件和文件夹，并提供恢复向导，网络管理员根据提示恢复即可。

提示：在恢复 Active Directory 域控制器中的文件时，建议使用“目录还原模式”，确保域控制器的安全。

（1）进入目录服务还原模式。重新启动计算机，在启动 Windows Server 2008 前，按 F8 键进入“高级启动选项”菜单界面。通过键盘上的方向键选择“目录服务还原模式”选项，如图 12-33 所示。

（2）按 Enter 键，加载操作系统文件，出现 Windows Server 2008 登录窗口，在用户名文本框中，输入 .\administrator 登录到本机，在密码文本框中，输入目录还原模式密码，如图 12-34 所示。






图 12-33 “高级启动选项”菜单界面　　图 12-34 Windows Server 2008 登录窗口

（3）启动完成，Windows Server 2008 系统处于安全模式，如图 12-35 所示。



图 12-35 Windows Server 2008 桌面

（4）依次选择“开始”→“管理工具”→Windows Server Backup 命令，打开 Windows Server Backup 窗口。

（5）在右侧“操作”面板中，单击“恢复”按钮，打开“入门”对话框。选择需要恢复的目标服务器，选中“此服务器”单选按钮，即恢复本地计算机。

（6）单击“下一步”按钮，显示“选择备份日期”对话框。选择已经备份成功的备份，选择备份内容以及备份时间。

（7）单击“下一步”按钮，显示图 12-36 所示的“选择恢复类型”对话框。在这里可以选中恢复“文件和文件夹”或“卷”单选按钮，根据需要进行选择即可，这里选中“文件和文件夹”

单选按钮。

（8）单击“下一步”按钮，显示图 12-37 所示的“选择要恢复的项目”对话框。在“可用项目”列表中，选择需要还原的目标文件夹，在右侧的列表中显示选择的文件夹中包含的文件，网络管理员可以选择一个文件或者多个文件。

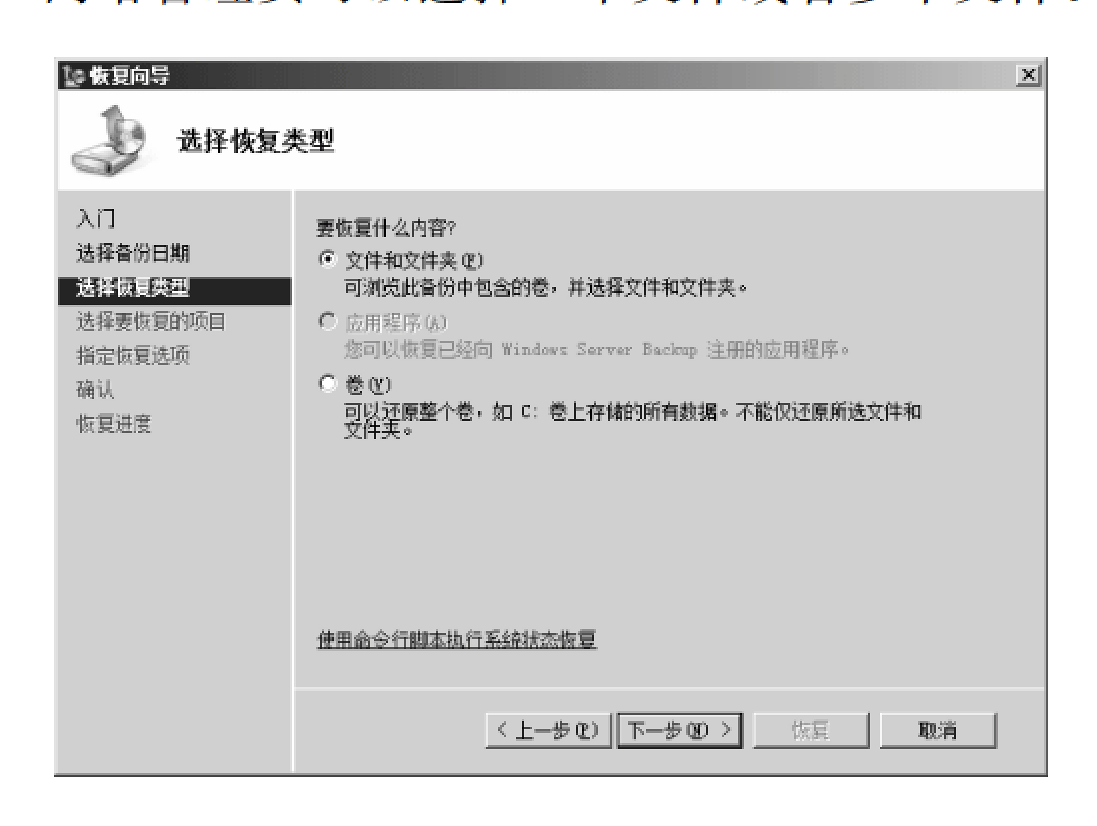


图 12-36　“选择恢复类型”对话框



图 12-37　“选择要恢复的项目”对话框

（9）单击“下一步”按钮，显示图 12-38 所示的“指定恢复选项”对话框。将选择文件恢复的目标文件夹，可以恢复到原始位置或者重定向到新的位置。如果在目标文件夹中已经存在同名文件时，网络管理员可以根据需要选择创建文件副本还是覆盖文件或者不恢复选择的文件夹。这里选中“另一个位置”单选按钮，并在其文本框中输入想要恢复到的文件夹，或单击“浏览”按钮，浏览恢复到的目标目录。

（10）单击“下一步”按钮，显示图 12-39 所示的“确认”对话框，显示恢复文件的“恢复目标”、“恢复选项”、“安全设置”等信息。

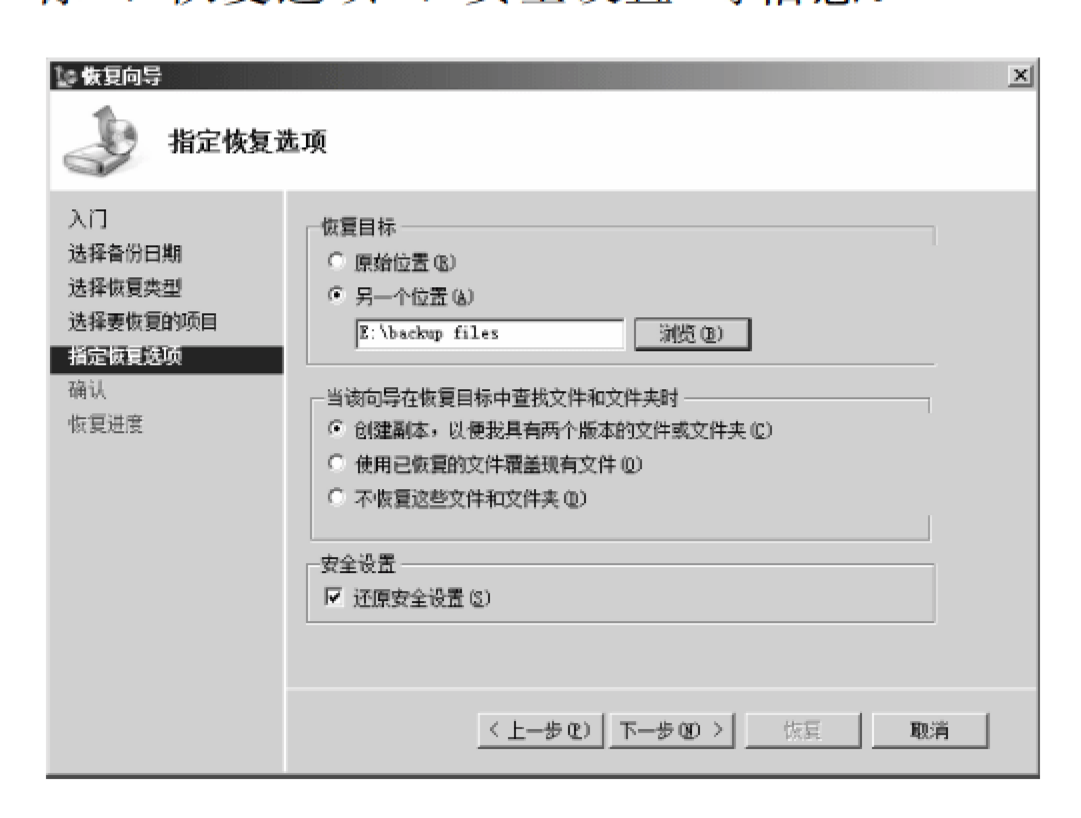


图 12-38　“指定恢复选项”对话框



图 12-39　“确认”对话框

（11）单击“恢复”按钮，即可执行文件恢复，恢复完成后，显示图 12-40 所示的“恢复进度”对话框。

（12）单击“关闭”按钮，完成文件恢复。

12.3.8　非权威还原

域控制器的系统状态还原必须在目录还原模式中进行，还原操作使用 Wbadmin.exe 命

令行完成。这里以恢复系统状态的方法为例。

(1) 在命令提示符中输入如下命令。

```
wbadmin get versions
```

按 Enter 键运行，查看 Active Directory 服务器备份列表，注意每次备份中的版本标识符，如图 12-41 所示。



图 12-40 “恢复进度”对话框



图 12-41 查看备份列表

(2) 在命令提示符中输入如下命令。

```
wbadmin start systemstaterecovery -version:12/05/2008-12:25
```

按 Enter 键运行，提示网络管理员是否要执行系统状态恢复，如图 12-42 所示。



图 12-42 提示是否执行恢复操作

(3) 输入 Y，即可开始执行恢复操作，如图 12-43 所示。

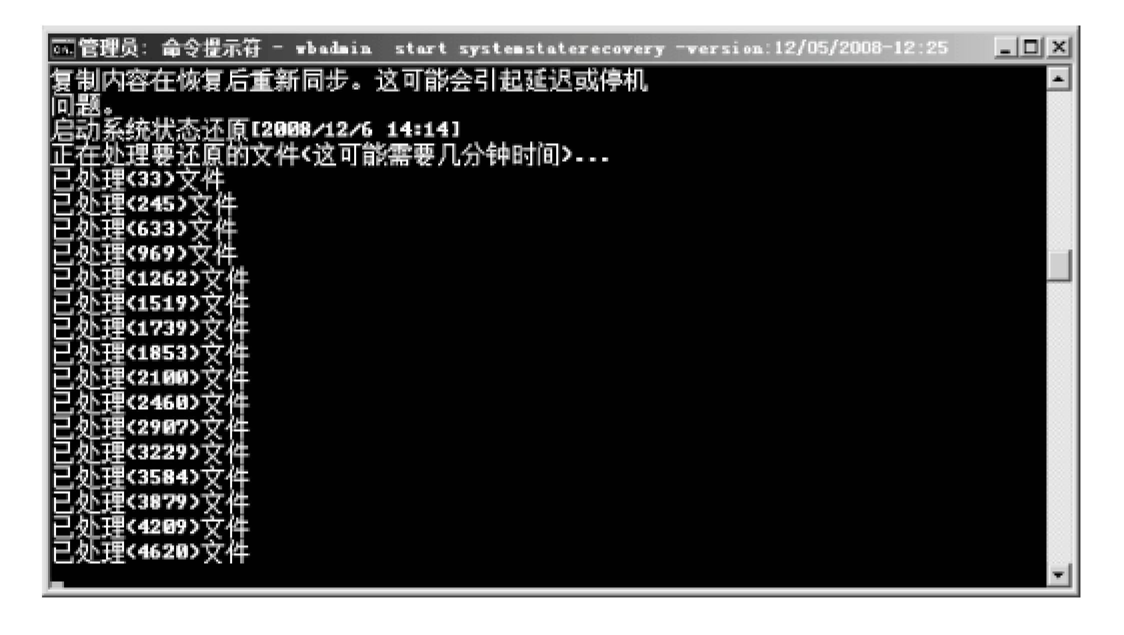


图 12-43 开始执行恢复

(4) 还原完成后，显示图 12-44 所示的窗口。



图 12-44　完成还原

(5) 重新启动服务器，在正常模式下登录 Windows Server 2008 活动目录，完成 Active Directory 数据库的还原即可。需要注意的是，在重新启动服务器时，将可能会多次重新启动计算机。服务器重启后，显示图 12-45 所示的提示框。



图 12-45　提示完成恢复

(6) 按 Enter 键，完成并关闭该窗口即可。

12.3.9　权威还原

在管理 Active Directory 的时候，网络管理员可能会错误地删除了一个不应该删除的用户或者组，如果使用同样的用户名称添加一个同名的用户，则以前的账户信息和其他的文件所有权信息会全部丢失，同时会禁止访问某些网络资源。

例如，网络管理员在维护 Active Directory 用户时，删除了 czc 用户，本例以“权威还原”模式恢复该用户。

(1) 进入“目录还原”模式，具体操作参见“非权威还原”，这里不再赘述。

(2) 在命令提示符中输入如下命令。

```
ntdsutil
```

(3) 在 ntdsutil 命令提示符中输入如下命令。

```
activate instance NTDS
```

按 Enter 键运行，激活 NTDSActive Directory 数据库实例，如图 12-46 所示。

(4) 在命令提示符中输入如下命令。

```
authoritative restore
```



图 12-46 激活 NTDSActive Directory 数据库实例

按 Enter 键运行。

(5) 在 authoritative restore 命令提示符中输入如下命令。

```
restore object cn=czc,ou=coolpen,dc=coolpen,dc=net
```

按 Enter 键运行,权威性地恢复已经删除的用户 czc,显示图 12-47 所示的"授权还原确认对话"对话框。

(6) 单击"是"按钮,开始执行恢复过程,执行完成后显示图 12-48 所示的运行结果。

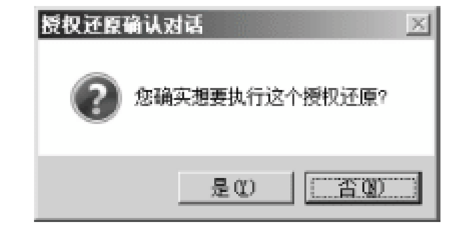


图 12-47 "授权还原确认对话"对话框



图 12-48 完成恢复

(7) 输入两次 quit,返回到命令行窗口,完成已经删除对象的恢复。

12.3.10 知识链接:活动目录数据库恢复

活动目录数据库恢复包括两种模式:非授权还原和授权还原。

1. 非授权还原

在同一个域中的域控制器之间随时都在同步数据,以保障所有域控制器中的数据都是相同的,当一台域控制器中产生新的数据时,这个变化就会同步到域中其他域控制器中。在网络中可能遇到这种情况,域控制器坏了,或者想要重新安装域控制器,可以先安装操作系统,然后恢复之前备份的数据库。恢复完成后,将自动和域中的其他域控制器同步,如果恢复后的域控制器的数据比较旧,其他域控制器自动将数据复制到该域控制器中,这种"自然"恢复称为"非权威还原"。

在正常还原操作中,备份会在非授权还原模式下执行。也就是说,要还原的所有数据,其中也包括活动目录对象,都将使用它们的原始更新序列号。所有未经授权还原的数据,都将在活动目录复制系统中出现,尽管数据是旧的。这就意味着数据不会复制到其他服务器。但如果其他服务器中出现较新的数据时,活动目录复制系统将会使用这些比较新的数据来

更新经过还原的数据。如果要将已还原的数据复制到其他服务器，必须使用授权还原模式。

2. 授权还原

在默认情况下，还原 Active Directory 数据库的模式为非授权还原，使用此方式还原 Active Directory 后，将从其他的域控制器中同步复制数据库。同步完成后，网络管理员会发现已经删除的用户没有被正常恢复，因为此用户的“墓碑记录”从其他服务器上被复制成功。当遇到这种情况的时候，可以使用 Active Directory 备份恢复没有删除用户的数据库，然后使用“授权还原”的方法禁止域中的其他域控制器复制同步 Active Directory 数据库，也就是说在网络中发布一个通告，新域控制器的数据是最高标准，其他所有域控制器都要以该域控制器为准，这样其他域控制器将不会将新的数据同步到该域控制器中。

要授权还原活动目录数据，需要在还原系统状态数据完成后，服务器重新启动之前运行 Ntdsutil 实用程序。当对象标记为授权还原时，会使其序列号比活动目录复制系统中的所有的更新序列号都要大，从而保证了所有还原的已复制或已分发的数据在本组织内得到正确的复制或分发。

习题

1. “最近一次的正确配置”适用于哪些情况？
2. “最近一次的正确配置”不适用于哪些情况？
3. 简述 Windows Server Backup 可完成的备份操作。

实验：备份并恢复服务器操作系统

实验目的：

掌握使用 Windows Server Backup 备份和恢复服务器操作系统的操作方法。

实验内容：

安装并使用 Windows Server Backup 备份操作系统，并使用备份文件进行恢复。需要注意的是，这里所进行的恢复操作，只是为了实验目的，在实际操作中通常不会连续进行恢复操作。

实验步骤：

（1）安装 Windows Server Backup。

（2）使用图形化界面进行完全备份。

（3）在服务器上创建一个测试用户。

（4）使用备份文件恢复操作系统。

（5）检查是否存在创建的测试用户。

第 13 章 chapter 13

网络设备故障的诊断与排除

在检查和定位网络故障时，必须认真地考虑一下可能出现故障的原因，以及应当从哪里开始着手，一步一步进行追踪和排除，直至最后恢复网络的畅通。

13.1 故障主要原因与现象

虽然故障现象千奇百怪，故障原因多种多样，但总的来讲就是硬件问题和软件问题，即网络连接性问题、配置文件和选项问题、网络协议问题及网络拓扑问题等。

1. 网络链路

网络链路是故障发生后首先应当考虑的原因。链路的问题通常是由网卡、跳线、信息插座、网线、交换机等设备和通信介质引起的。其中，任何一个设备的损坏，都会导致网络连接的中断。链路通常可采用软件和硬件工具进行测试验证，例如，当某一台计算机不能浏览Web时，首先想到的就是网络链路的问题。到底是不是呢？这要通过测试进行验证。FTP可以登录吗？看得到网上邻居吗？可以收发电子邮件吗？Ping得到网络内同一网段的其他计算机吗？只要其中一项回答为"YES"，那就不是链路问题。当然，即使回答为"NO"，也不就表明链路肯定有问题，而是可能会有问题，因为如果计算机网络协议的配置出了毛病也会导致上述现象的发生。另外，看一看网卡和交换机的指示灯是否闪烁及闪烁是否正常。

当然，如果排除了由于计算机网络协议配置不当而导致故障的可能后，接下来要做的事情就比较麻烦了。查看网卡和交换机的指示灯是否正常，测量网线是否通畅，检查交换机的安全配置和VLAN配置，直至最后找到影响网络链路的原因。

2. 配置文件和选项

所有的交换机和路由器都有配置文件，所有的服务器、计算机都有配置选项，而其中任何一台设备的配置文件和配置选项设置不当，同样会导致网络故障，例如，路由器的访问列表配置不当，会导致Internet连接故障；交换机的VLAN设置不当，会导致VLAN间的通信故障，彼此之间都无法访问，更不用说访问Internet了；服务器权限的设置不当，会导致资源无法共享或无法获得足够权限的故障；计算机网卡配置不当，会导致无法连接的故障等。因此，当排除硬件故障之后，就需要重点检查配置文件和选项的故障了。当某一台计算机无法接入网络时，或者无法同连接至同一交换机的其他计算机通信时，应当检查接入交换机的配置；当某台接入层交换机无法连接至网络时，应当检查该交换机级联端口以及汇聚层交换机的配置；当同一VLAN或几个VLAN内的交换机无法访问时，应当检查接入、汇

聚或核心交换机的配置；当所有交换机都无法访问 Internet 时，就应当检查路由器或代理服务器的配置；当个别服务无法实现时，应当检查提供相应服务的服务器配置。

3. 网络协议

网络协议其实就是在网络设备和计算机网络中彼此“交谈”时所使用的语言。因此，说没有网络协议就没有网络这句话一点都不过分。没有网络协议，网络内的网络设备和计算机之间就无法进行通信，所有的硬件设备也不过都是一堆摆设而已。这就和“没有操作系统和应用软件，计算机就是一具没有灵魂的躯壳”是一个道理。因此，网络协议的配置在网络中居于举足轻重的地位，决定着网络能否正常运行。网络协议的含义非常广泛，既包括交换机和路由器执行的网络协议，也包括计算机和路由器执行的网络协议。其中任何一个协议配置不当或没有正常工作，都有可能导致网络瘫痪或导致某些服务被终止，从而出现网络故障。

4. 网络服务故障

网络服务故障主要包括 3 个方面，即服务器硬件故障、网络操作系统故障和网络服务故障。所有的网络服务都必须进行严格的配置或授权，否则，就会导致网络服务故障，例如，服务器权限的设置不当，会导致资源无法访问的故障；主目录或默认文件名指定错误，会导致 Web 网站发布错误；端口映射错误，会导致无法提供某种服务；等等。因此，当排除硬件故障之后，就需要重点检查配置文件和选项的故障了。当企业网络内所有的服务都无法实现时，应当检查网络设备的配置，尤其是连接网络服务器的交换机的配置；如果只有个别服务无法实现时，则应当检查提供相应网络服务的相关配置。

13.2 网络故障排除过程

在开始动手排除故障之前，建议先准备一支笔和一个笔记本，将故障现象认真仔细地记录下来。也就是说，应当养成一种良好习惯，在开始着手进行排除故障时就开始做笔记，而不是在事情做完之后才来做。认真而翔实地记录不仅有助于一步一步地记录问题、跟踪问题并最终解决问题，而且，也为自己或同事以后解决类似问题时提供完整的技术文档和帮助文件。注意，在观察和记录时一定要注意细节。

1. 识别故障现象

网络管理员在进行故障排除之前，必须确切地知道网络上到底出了什么问题，是不能共享资源，还是不能浏览 Web 页，或是不能聊 QQ，等等。知道出了什么问题并能够及时识别是成功排除故障最重要的步骤。对一名优秀网络管理员的最基本要求，首先就是对问题进行快速定位，也就是说，能够及时找到处理问题的出发点。

为了与故障现象进行对比，必须非常清楚网络的正常运行状态。作为网络管理员，如果系统在正常情况下是怎样工作的都不知道，那么又怎么能够对问题和故障进行定位呢？因此，了解网络设备、网络服务、网络软件、网络资源在正常状态下的表现方式，了解网络拓扑结构、理解网络协议、掌握操作系统和应用程序，都是故障排除必不可少的理论和知识准备。再次强调，在识别故障现象之前，必须明确了解网络系统的正常运行特性。

识别故障现象时，应该询问以下几个问题。

（1）当被记录的故障现象发生时，正在运行什么进程？

(2) 这个进程以前运行过吗?

(3) 以前这个进程的运行是否成功?

(4) 这个进程最后一次成功运行是什么时候?

(5) 故障现象是什么?

2. 对故障现象进行详细描述

当处理由用户报告的问题时,对故障现象的详细描述显得尤为重要。当网络管理员接到用户电话说无法浏览 Web 网站,如果仅凭这些消息,恐怕任何人都无法做出明确的判断。这时,就要亲自到现场去试着操作,运行一下那个程序,并注意出错信息,例如,在使用 Web 浏览器进行浏览时,无论输入哪个网站都返回“该页无法显示”之类的信息;或者使用 Ping 程序时,无论 Ping 哪个 IP 地址都显示超时连接信息等,诸如此类的出错消息会为缩小问题范围提供许多有价值的信息。注意每一个错误信息,并在用户手册中找到它们,从而得到关于该问题更详细的解释,是解决问题的关键。另外,亲自到故障现场进行操作,也有机会检查用户操作系统或应用程序是否运行正常,各种选项和参数是否被正确地设定。如果在操作时没有任何问题,那就可能是操作者的问题了。不妨让用户再试一次,并认真监督他的每一步操作,以确保所有的操作和选项都被正确地执行和设置。

当然,在亲自操作时,应当对故障现象做出详细的描述,认真记录所有的出错信息,并快速记录所有有关的故障迹象,制作详尽的故障笔记。在寻找问题答案的过程中,很有可能又导致更多的故障现象产生。所以在开始排除故障之前,应按以下步骤执行。

(1) 收集有关故障现象的信息。

(2) 对问题和故障现象进行详细的描述。

(3) 注意细节。

(4) 把所有的问题都记下来。

3. 列举可能导致错误的原因

接下来要做的就是列举所有可能导致故障现象的原因了。网络管理员应当考虑导致无法使用 Web 浏览器的原因可能有哪些,如网卡硬件故障、网络连接故障、网络设备故障、TCP/IP 协议设置不当等。在这个阶段不要试图去确定哪一个原因就是问题的所在,只要尽量多地记录下自己所能想到的,而且是可能导致问题发生的原因就可以了。或许可以根据出错的可能性把这些原因按优先级别进行排序。注意,千万不要忽略其中的任何一个细节。

4. 缩小搜索范围

网络管理员必须采用有效的软硬件工具,从各种可能导致错误的原因中一一剔除非故障因素。对所有列出的可能导致错误的原因逐一进行测试,而且不要根据一次测试,就断定某一区域的网络是运行正常或是不正常。另外,也不要在自己认为已经确定了的头一个错误上停下来,而不再继续测试。因为此时既可能是搞错了,也有可能存在的错误不止一个。所以,应该使用所有可能的方法来测试所有的可能性。

除了测试之外,还要注意做以下几件重要的事情。

(1) 查看网卡、交换机和路由器面板上的 LED 指示灯。通常情况下,绿灯表示连接正常;红灯表示连接故障;不亮表示无连接或线路不通;长亮表示可能存在广播风暴;指示灯有规律地闪烁才是网络正常运行的标志。

（2）查看服务器、交换机或路由器的系统日志，因为在这些系统日志中，往往记载着产生的错误以及错误发生的全部过程。

（3）如果有幸拥有并安装了诸如 CiscoWorks、HP OpenView 之类的网络管理软件，千万不要忘记用它们来检查一下哪些设备出现了问题。由于这些网络管理软件往往具有图形化的用户界面，因此，交换机各端口的工作状态可以一目了然地显示在屏幕上。更进一步，许多网络管理软件还具有故障预警和报警功能，从而使在缩小搜索范围时省下不少的力气。

当然，在这一步骤中最不能忘记的还是要记录下所有观察及测试的手段和结果。

5. 隔离错误

网络管理员经过反复地测试，此时也搞清楚了到底是哪一部分故障导致了问题的发生，并最终确定很有可能是计算机出错了。于是，便开始检查该计算机网卡是否安装好、TCP/IP 协议是否安装并设置正确、Web 浏览器的连接设置是否得当等一切与已知故障现象相关的内容。然后，剩下的事情就是排除这个故障了。此时，由于对所发生的故障已经有了充分的了解，因此，故障排除也就手到擒来了。但是，不要就此匆忙地结束工作，因为还有更重要的事情等着去做。

6. 故障分析

处理完问题之后还有什么要做的呢？作为网络管理员必须搞清楚故障是如何发生的，是什么原因导致了故障的发生，以后如何避免类似故障的发生，拟定相应的对策，采取必要的措施，制定严格的规章制度。

对于一些非常简单明显的故障，上述过程看起来可能会显得有些烦琐。但对于一些复杂的问题，这却是必须遵循的操作规程。

最后，记录所有的问题，保存所有的记录。另外，经常回顾曾经处理过的故障也是一种非常好的习惯，这不仅是一种经验的积累，便于以后处理类似故障，而且还会启发思考许许多多与此相关联的问题，从而进一步提高理论和技术水平。

13.3　故障诊断与排错

在故障发生时，作为一名合格的管理员，必须能够清楚地对故障进行诊断，并使用相应的措施排除故障。从故障发生时所表现的状况着手进行分析，确认故障排除方案，并最终排除故障。

13.3.1　链路故障

当一台正常连接的服务器突然无法提供服务时，链路故障的可能性非常大。统计表明，链路故障在网络故障总量中约占有 80%的比重，因此，链路故障是网络中最常发生的故障之一。通常情况下，虽然链路故障的表现形式比较多，但由于便于观察和测试，因此，解决起来却往往并不困难。

1. 链路故障的表现

链路故障通常表现为以下几种情况。

（1）计算机无法登录至服务器。

（2）计算机在网上邻居中只能看到自己，而看不到其他计算机，从而无法使用其他计算

机上的共享资源和共享打印机。

(3) 计算机无法通过局域网接入 Internet。

(4) 计算机无法在局域网络浏览 Web 服务器,或进行 E-mail 收发。

(5) 网络中的部分计算机运行速度十分缓慢。

2. 链路故障的分析

以下原因可能导致链路故障。

(1) 网卡未安装,或未正确安装,或与其他设备有冲突。

(2) 网卡硬件故障。

(3) 网络协议未安装,或设置不正确。

(4) 网线、跳线或信息插座故障。

(5) UPS 故障。

(6) 交换机电源未打开,交换机硬件故障,或交换机端口硬件故障。

(7) VLAN 设置问题。

3. 链路故障的排错步骤

当计算机出现以上链路故障现象时,通常建议按照以下步骤进行故障的定位与排错。

(1) 确认链路故障

当出现一种网络应用故障时,如无法接入 Internet,首先尝试使用其他网络应用,如查找网络中的其他计算机,或使用局域网络中的 Web 浏览,等等。如果其他网络应用可正常使用,如虽然无法接入 Internet,却能够在网上邻居中发现其他计算机,或可 Ping 到其他计算机,可排除链路故障原因。如果其他网络应用均无法实现,继续下述步骤。

(2) 基本检查

查看网卡的指示灯是否正常。正常情况下,在不传送数据时,网卡的指示灯闪烁较慢,传送数据时,闪烁较快。无论是不亮,还是长亮不灭,都表明有故障存在。如果网卡的指示灯不正常,需关掉计算机更换网卡。如果指示灯闪烁正常,继续下述步骤。

(3) 初步测试

使用 ping 命令,Ping 本地的 IP 地址或 127.0.0.1,检查网卡和 IP 网络协议是否安装完好。如果能 Ping 通,说明该计算机的网卡和网络协议设置都没有问题,问题出在计算机与网络的连接上。因此,应当检查网线的链路和交换机及交换机端口的状态。如果无法 Ping 通,只能说明 TCP/IP 协议有问题,而并不能提供更多的情况。因此,需继续下述步骤。

(4) 排除网卡

在“控制面板”的“系统”窗口中,查看网卡(网络适配器)是否已经安装或是否出错。如果在系统中的硬件列表中没有发现网络适配器,或网络适配器前方有一个黄色的“!”,说明网卡未安装正确,需将未知设备或带有黄色“!”的网络适配器删除,刷新后,重新安装网卡。并为该网卡正确安装和配置网络协议,然后进行应用测试。如果网卡无法正确安装,说明网卡可能损坏,必须换一块网卡重试。如果网卡已经正确安装,继续下述步骤。

(5) 排除网络协议故障

使用 ipconfig /all 命令查看本地计算机是否安装有 TCP/IP 协议,以及是否设置好 IP 地址、子网掩码和默认网关、DNS 域名解析服务。如果尚未安装协议,或协议尚未设置好,

安装并设置好协议后，重新启动计算机，执行步骤(2)的操作。如果已经安装，认真查看网络协议的各项设置是否正确。如果协议设置有错误，修改后重新启动计算机，然后再进行应用测试。如果协议设置完全正确，则肯定是网络连接的问题，继续执行下述步骤。另外，若欲使用局域网络中的“网上邻居”，应安装 NetBEUI 协议。

(6) 故障定位

到连接至同一台交换机上的其他计算机上进行网络应用测试。如果仍不正常，在确认网卡和网络协议都正确安装的前提下，可初步认定是交换机发生了故障。为了进一步进行确认，可再换一台计算机继续测试，进而确定交换机故障。如果其他计算机测试结果完全正常，则将故障定位在发生故障的计算机与网络的链路上。

(7) 故障排除

如果确定交换机发生了故障，应首先检查交换机面板上的各指示灯闪烁是否正常。如果所有指示灯都在非常频繁地闪烁，或一直亮着，可能是由于网卡损坏而发生了广播风暴，关闭再重新打开交换机电源后试一试看能否恢复正常。如果恢复正常，再找到红灯闪烁的端口，将网线从该端口中拔出。然后找到该端口所连接的计算机，测试并更换损坏的网卡。如果面板一片漆黑，一个灯也不亮，那也不要过于担心，检查一下 UPS 是否工作正常，交换机电源是否已经打开，或电源插头是否接触不良。如果电源没有问题，那恐怕就得更换一台交换机了。

如果确定故障就发生在某一条连接上，做起来就稍微麻烦些。首先，测试、确认并更换有问题网卡。其次，用网线测试仪对该连接中涉及的所有网线和跳线进行测试，确认网线的链路正常。如果问题就出在这儿，那就简单了，重新制作网头或更换一条网线就行了。最后，检查交换机相应端口的指示灯是否正常，再换一个端口试试。

13.3.2　协议故障

没有协议就没有网络。如果说人与人之间的情感交流、思想沟通需要通过语言来实现，那么，计算机和网络设备之间的通信就要靠协议来实现。协议之于网络正如同语言之于人类，因此，协议在网络中扮演着非常重要的角色。协议故障的表现在许多方面与链路故障有相似之处，但在分析和判断时，却要比链路故障简单得多，解决起来也容易得多。既无须借助于过多的软件工具，更无须借助任何硬件工具，只需要使用 Ping 命令即可。

1. 协议故障表现

协议故障通常表现为以下几种情况。

(1) 计算机无法登录至服务器。

(2) 计算机在网上邻居中既看不到自己，也看不到其他计算机或查找到其他计算机。

(3) 计算机在网上邻居中能看到自己和其他计算机，但无法在局域网络中浏览 Web 页面、收发 E-mail。

(4) 计算机在网上邻居中既看不到自己，也无法在局域网络中浏览 Web 页面、收发 E-mail。

(5) 计算机无法通过局域网接入 Internet。

(6) 与网络中其他计算机的名称重复，或者与其他计算机使用的 IP 地址相同。

2. 协议故障分析

以下原因可能导致协议故障。

(1) 协议未安装。实现局域网网络通信,需安装 NetBEUI 协议;实现 Internet 通信,需安装 TCP/IP 协议。

(2) 协议配置不正确。TCP/IP 协议涉及的基本配置参数有 4 个,即 IP 地址、子网掩码、DNS(域名解析服务)和默认网关,任何一个设置错误,都会导致故障发生。

(3) 网络(VLAN)中有两个或两个以上的计算机使用同一计算机名称。

3. 协议故障排错步骤

当计算机出现以上协议故障现象时,应当按照以下步骤进行故障的定位与排错。

(1) 检查计算机是否安装有 TCP/IP 协议,如果没有,建议安装该协议,并重新启动计算机。

(2) 检查计算机的 TCP/IP 配置参数是否正确。如果设置有问题,修改后重新启动计算机,并再次测试。否则,将无法浏览 Web 页面和收发 E-mail,也无法享受网络提供的其他 Intranet 或 Internet 服务。

(3) 使用 Ping 命令,测试与其他计算机和服务器的连接状况。

(4) 在"控制面板"的网络属性窗口中,单击"文件及打印共享"按钮,在显示的"文件及打印共享"对话框中检查是否选中了"允许其他用户访问我的文件"和"允许其他计算机使用我的打印机"复选框,或者它们两个之中的一个。如果没有,全部选中,或选中一个,否则,将无法使用共享文件夹。

(5) 系统重新启动后,稍待片刻,双击"网上邻居"图标,显示网络中的计算机和共享资源。如果仍看不到其他计算机也不要灰心,使用"查找"功能搜索网络中的已知计算机,或者按 F5 键对整个系统刷新,这时就会惊喜地发现所有的一切都来了。

(6) 在网络属性窗口的"标识"文本框中重新为该计算机命名,使其在网络中具有唯一性。计算机名不超过 17 个字符,且不得包含空格。可见,校园网络中心不仅要负责 IP 地址和域名的分配与管理,而且也要负责计算机名称的分配与管理,否则,将导致"天下"大乱。当然,由于 NetBEUI 不具有路由功能,所以,在不同的 VLAN 中,计算机是可以重名的。

13.3.3 配置故障

配置错误也是导致故障发生的重要原因之一。网络管理员对服务器、交换机、路由器的不当设置自然会导致网络故障,计算机使用者(特别是接触计算机时间不长的用户)对计算机设置的修改,也往往会产生一些令人意想不到的访问错误。配置故障更多的时候是表现在不能实现网络所提供的各种服务上,如不能接入 Internet,不能访问某种代理服务器等,与链路故障在表现上会有较大差别。在故障的调查、分析和测试过程中,只要稍加留意,就会很容易地发现故障原因。服务器和网络设备的配置往往需要较多的理论知识和较高的技术水平。因此,在修改配置前,必须做好原有配置的记录,并最好进行备份。

1. 配置故障表现

配置故障通常表现为以下几种情况。

(1) 网络链路测试正常,却无法连接到网络,不能与其他计算机通信。可能是接入交换机的某个端口配置错误,也可能是用户的 IP 地址信息配置错误。

(2) 只能与某些计算机,而不是全部计算机进行通信。可能是接入交换机配置错误,也可能是三层交换机配置错误。

（3）计算机只能访问内部网络中的服务器，但无法接入 Internet。可能是路由器配置错误，也可能是三层交换机配置错误，或者是代理服务器配置错误。

（4）计算机无法通过代理服务器接入 Internet。可能是代理服务器配置错误，也可能是用户端应用程序的代理服务器信息设置错误。

（5）计算机无法登录至域控制器。可能是域控制器设置错误，也可能是客户端没有正确添加至域。

（6）计算机无法访问任何其他设备。可能是没有正确安装网卡驱动程序、网络协议，或者是没有正确设置 IP 地址信息。

2. 配置故障分析

以下原因可能导致配置故障。

（1）服务器配置错误，例如，域控制器未设置或已到期的用户，将无法登录；服务器配置错误导致 Web、E-mail 或 FTP 服务停止；代理服务器访问列表设置不当，将阻止有权用户接入 Internet。

（2）网络设备配置错误，例如，路由器访问列表设置不当，不仅会阻止有权用户接入 Internet，而且还会导致网络中所有计算机都无法访问 Internet；第三层交换机的路由设置不当，用户将无法访问另一 VLAN 中的计算机；当交换机设置有安全端口后，非授权用户对该端口的访问，将导致端口锁死，从而导致该端口所连接的计算机无法继续访问网络；VLAN 或 VLAN Trunk 设置不当，也会导致某台或某些计算机无法连接到核心网络。

（3）用户配置错误，例如，IP 地址信息设置错误（特别是子网掩码或默认网关设置错误）；Internet Explorer 浏览器的“连接”设置不当，用户将无法通过代理服务器接入 Internet；邮件客户端的邮件服务器设置不当，用户将无法收发 E-mail。

3. 配置故障排错步骤

配置故障排错步骤如下。

（1）检查发生故障计算机的相关配置。如果发现错误，修改后，再测试相应的网络服务能否实现。如果没有发现错误，或相应的网络服务不能实现，执行下述步骤。

（2）测试同一网络内的其他计算机是否有类似的故障，如果有同样故障，说明问题肯定出在服务器或网络设备上。

（3）如果没有类似故障，也并不能排除服务器和网络设备存在设置问题的可能性，也应针对为该用户提供的服务做认真的检查。

13.3.4　服务器故障

导致网络服务故障的可能性包括 3 个方面，即服务器硬件故障、操作系统故障和网络服务故障。通常情况下，导致网络故障最主要的原因是操作系统故障，因此，当网络服务故障发生时，首先应当确认服务器是否感染病毒或被攻击。

1. 操作系统故障

服务器操作系统是为 7×24 不间断运行设计的，因此，可以长期稳定地正常运行，通常不会出现蓝屏、速率变低、系统瘫痪等客户端操作系统常见的系统故障。然而，服务器操作系统本身也存在着许多系统和安全漏洞，非常容易招致蠕虫病毒或其他各种恶意攻击。

(1) 病毒侵袭

蠕虫是一种通过网络传播的恶性病毒,它具有病毒的一些共性,如传播性、隐蔽性、破坏性等;同时具有自己的一些特征,如不利用文件寄生(有的只存在于内存中),对网络造成拒绝服务,以及和黑客技术相结合等。网络的发展使得蠕虫可以在短短的时间内蔓延整个网络,造成网络传输速率大幅下降,甚至导致网络瘫痪,因此,对企业网络极具破坏性和杀伤力。

可采取以下方式防范病毒攻击。

① 只提供网络服务。除非维护需要,否则,不要直接对服务器进行操作,更不要将服务器作为普通计算机使用,随意使用服务器浏览 Web 网站、收发电子邮件,以避免由于访问恶意网页或邮件而感染病毒。

② 关闭不需要的服务。关闭或删除系统中不需要的服务,只打开网络服务所必须使用的端口。提供的服务和打开的端口越少,可被利用的安全漏洞也就越少,服务器就越不容易被恶意攻击,也就越安全。

③ 安装系统补丁。绝大多蠕虫病毒都是利用系统漏洞进行传播的,因此,一定要将服务器设置为自动下载并安装系统升级包,实时访问微软的 Windows Update 网站,及时下载并安装 Windows 系统(包括应用程序)安全补丁。

④ 安装病毒防火墙。仅有系统安全补丁是不够的,还必须安装专业的防病毒软件,并打开防病毒软件的实时监控功能,及时发现并清除(或隔离)已经感染的病毒。另外,应当及时升级防病毒程序的病毒库和引擎,以确保能够识别并清除最新发现的病毒。

(2) 磁盘空间太小

作为网络服务器,往往需要 2GB 以上的空间用于存储临时文件。当剩余的硬盘空间较少时,将严重影响服务器的性能,使响应速度变慢,严重时甚至会导致系统瘫痪。因此,一定要将系统分区与数据分区分开,一方面可以保证数据不会因为系统故障而丢失;另一方面也可以保证系统分区始终拥有足够的剩余空间。

(3) 垃圾文件过多

系统和网络服务在正常运行过程中会产生一些临时文件、垃圾文件和磁盘碎片。正常情况下,临时文件会被系统自动删除。然而,在非正常关机或应用程序非正常退出时,临时文件将不会被删除掉。随着使用时间的延长,垃圾文件会越来越多,除了会大量占用宝贵的硬盘空间外,还将导致系统运行速度变慢,甚至导致系统瘫痪。因此,应当定期执行系统工具中的“磁盘清理”,彻底清除不再使用的临时文件和垃圾文件。

(4) 蓝屏故障原因及解决方法

虽然现在服务器操作系统的稳定性得到了很大的提高,但仍有发生蓝屏的情况出现,因此,如何解决蓝屏的问题也是日常管理的工作之一。导致蓝屏故障的原因非常多,CPU 过热或内存故障、系统硬件冲突、系统缺陷、病毒或黑客攻击、注册表中存在错误或损坏、启动时加载程序过多、程序版本冲突、虚拟内存不足造成系统多任务运算错误、动态链接库文件丢失、系统资源冲突或资源耗尽等都会产生蓝屏。另外,软硬件存在冲突也很容易出现蓝屏现象。

借助于以下措施,可以有效地消除蓝屏。

① 系统扩容时,优先选用同一厂商的产品,以保证系统之间的硬件兼容性。

② 了解产品的进货渠道,确保产品质量。

③ 安装空气调节系统，确保服务器能够及时、有效地散热。

④ 减少系统启动时的自动加载程序。随系统启动的程序过多，既影响系统启动速度，又占用各项资源，因此，在系统启动时，应当只加载服务所必需的程序。

⑤ 删除多余的 DLL 文件。在 Windows 操作系统的 System 子目录里有许多的 DLL 文件，这些文件可能被许多文件共享，但有的却没有一个文件要使用它，也就是说这些文件没用了，为了不占用硬盘空间和提高启动运行速度，完全可以将其删除。但为防止误删除文件，特别是比较重要的核心链接文件，可用工具软件如“超级兔子”对无用的 DLL 文件进行删除，这样可防止误删除文件。

⑥ 扩大虚拟内存容量。虚拟内存是 Windows 系统所特有的一种解决系统资源不足的方法，一般要求为物理内存的 2～3 倍。虚拟内存过小将容易出现蓝屏，因此，必须保证虚拟内存的容量。

⑦ 安装系统补丁和安全补丁，使操作系统处于最佳工作状态。

2. 网络服务故障

由于操作系统 Bug、应用程序缺陷、内存质量、硬盘可靠性等各种不可预知的因素，有时会导致网络服务中断。

当网络服务故障发生时，通常都会在系统日志中有记载，可以通过“管理工具”→“事件查看器”窗口查看。通常情况下，系统故障会记录在“系统”文件夹中，如果是应用程序或非 Windows 内置的网络服务发生故障，则会记录在“应用程序”文件夹中。

当发生网络故障时，可以采用以下几个步骤进行处理。

(1) 重新启动服务。依次打开“管理工具”→“服务”窗口，右击已经发生故障的服务，选中“启动”或“重新启动”单选按钮。如果网络服务通过其他控制台管理，也可在相应的控制台中重新启动。

(2) 重新启动计算机。当重新启动服务仍然无法正常实现网络服务时，可以选择重新启动计算机，清除计算机内存重新加载网络服务。

(3) 重新安装服务或应用程序。如果重新启动计算机仍然不能排除故障，可以考虑卸载并重新安装相应的 Windows 组件或应用程序。

3. 服务器硬件故障

由于服务器本身在硬件选用上非常严格，所以，通常情况下，在非人为干预情况下，发生服务器故障的可能性比较小。所以，硬件故障往往是在安装新的板卡、修改系统配置文件，或者进行扩容后发生的。

当扩容后发生硬件故障时，应当执行下述操作。

(1) 检查扩容部件。去掉新增加内存、CPU 或第三方 I/O 卡，检查硬盘、软驱、光驱的信号线有没有接反，跳线是否正确。

(2) 拔除扩展卡。拔除可能导致故障发生的板卡，直至故障恢复。

(3) 检查板卡连接。检查内存、CPU 或其他板卡插得是否牢靠，必要时拔下重新安装。

当安装硬件驱动程序后发生故障，应当执行下述操作。

(1) 采用安全模式。如果系统无法正常引导，可以在系统启动时，按 F8 键，选择“安全模式”选项，只加载必须的硬件设备。然后，依次打开“管理工具”→“计算机管理”窗口，删除新安装的硬件。

（2）恢复系统。利用系统恢复功能，将系统恢复至安装新硬件前的状态。

（3）升级驱动程序。先从设备厂商的官方网站下载最新的驱动程序，然后，进入“计算机管理”窗口，右击发生故障的硬件设备，选择“更新驱动程序”命令，升级该设备的驱动程序。

13.3.5 网络拓扑故障分析

一般情况下，在网络的设计之初，网络设计者们都已经将网络的各种功能基本上发挥到了一定的程度，同时也已经考虑到了某些故障，并会做出一些相应的措施来避免故障的发生。但作为一名合格的网络工程师，应该同时做出相应的解决方案。一般在网络初次建好后是不会出现故障的，因为在网络建好后，网络设计者已经将各种网络设备的设置、网络设备的连接做好了，并已经完成了种种调试和测试。

因为网络拓扑所引起的故障多数情况下是由于网络管理人员对网络的结构模糊，或者对网络拓扑结构进行某些操作所造成的，所以对于网络拓扑结构来说其故障一般是人为造成的。其网络拓扑结构故障一般表现为更改网络拓扑结构，对网络拓扑结构进行优化。网络拓扑结构的更改，主要是由于对网络设备的重新配置而改变了网络的拓扑结构，以及在网络的主要结构中加入了新的网络设备而改变了网络拓扑结构。网络拓扑结构的优化故障主要是由于网络管理人员对网络内的设备，包括交换机、路由器，进行了重新配置，使其能够最大限度地提供服务，而最终造成的故障。

1. 更改拓扑结构导致网络故障

由于局域网中的网络拓扑结构相对来说是比较稳定的，一般不会像笔记本电脑一样，位置可以随意改变。但这并不能说，网络拓扑结构是一定不能改变的，但需要注意的是，在更改自己的网络拓扑结构之前，必须对需要更改的网络拓扑结构有一个比较详细的了解，必须根据现有的网络拓扑结构进行更改。

建议每个网络管理人员都要备份一份甚至多份所管理的网络的拓扑结构图，这样做的目的就是在网络出现故障时，能够轻松地查找故障的原因。另一方面，在升级网络时可以避免出现一些本来可以避免的故障。

随着技术的发展，所使用的网络都会面临着升级，这里所说的升级，不单单说的是网络设备的升级，还包括网络拓扑结构和网络软件的升级等。所以保证网络的可升级性在网络的设计之初也是一项必不可少的工作。网络升级和扩展的空间，是判断网络好坏的一个重要指标。因此在升级网络前，应首先考虑网络的升级空间到底有多大，如果在升级网络时，完全不管网络的可升级性，而对网络盲目地添加设备、盲目升级，有可能会在升级网络后，而产生一些莫名其妙的故障，从而最终使用户吃亏。

故障实例解析如下。

某单位的网络主要分为两部分，一部分是由一些老计算机和集线器组成的局域网，一部分是由一些新计算机和交换机组成的局域网。一开始两部分的网络是互相独立的，两个局域网之间并不能进行通信，现在为了使所有的计算机都能够互访，便使用一根双绞线将交换机与集线器连接在了一起，但连接后的结果并不像开始所想象的那样两部分的网络计算机可以实现互相之间的信息通信，而是一部分计算机之间可以实现信息通信，剩余部分的计算机之间却不能进行通信，从而造成网络故障的发生。

既有交换机也有集线器混合构建的网络叫做混合网络，因为在网络中由于计算机数量比较多，所以很容易使网络传输产生碰撞而影响正常访问。另外，由于交换机和集线器本身工作原理的不同，也使得交换机在传输带宽和传输效率方面都比集线器要高很多。也正是这个原因，如果直接将交换机和集线器连接在一起工作，因为其工作效率是不相同的，所以会很容易产生网络通信故障。这里所发生的故障也正是由于这个原因所造成的，因此如果想要解决该网络的故障，必须从故障的根源上着手，也就是前面所说的更改网络的网络拓扑结构。

对于混合网络，应当把其中一台性能最好的交换机作为网络的中心，其他交换机、集线器、服务器、打印机等设备都连接至该交换机，而普通计算机则连接至集线器。

这种方式以交换机端口将各集线器的碰撞域分隔开来，有效地减少了网络碰撞冲突，大幅度提高了网络传输效率。由于服务器和打印机等各用户频繁访问的设备都连接至交换端口，拥有较高的网络带宽，从而解决了网络的传输瓶颈。

2. 拓扑结构优化造成网络故障

对网络拓扑结构的优化是指对已经正式投入使用的网络结构进行分析，并找出影响网络运行的原因，并且通过采取某些网络技术手段优化网络，从而达到优化网络的运行状态，充分利用资源等的目的。尽管每个网络在开始设计之初，已经考虑得十分周密，但随着时间的推移，设备的不断更新以及新计算机的购买，原来所规划的网络已经不能再满足所要求的应用和需求，此时对网络进行优化就成为确保网络的首选。

（1）网络拓扑结构的优化

由于建网时的资金限制、网络扩展等原因，而使网络结构设计不合理、设备使用不合理，从而导致网络使用效率低、设备负担不合理、网络运行不稳定等现象产生。可以通过优化网络结构得到改善，以提高网络资源的利用率。对网络拓扑结构进行优化的多数网络都属于大、中型网络，而在这些网络中一般采用三层网络设计模型，分别为核心层、汇聚层和接入层。

在实际的优化过程中由于三层结构的不同功能，优化的重点主要为保证核心层的高速、稳定、可靠性；汇聚层的可扩展性；接入层的可管理性。

在网络拓扑结构优化过程中，应根据网络的实际需求选择合适的拓扑结构。在传统的网络拓扑布线时，为了减少线路成本，比较多地采用节点汇聚的方式，而现在随着网络介质成本的降低、维护成本的增加，网络设计者更多地考虑减少节点或者是减少有源节点的方式，将汇聚层直接设置在大楼内部，从核心到汇聚都采用直接逻辑连接，不再设置中间有源节点。这种方式主要对用户较多、网络应用较多、路由协议复杂的大规模网络比较适合。

（2）VLAN 的规划

LAN 可以是由少数几台计算机构成的网络，也可以是数以百计的计算机构成的企业网络。VLAN（Virtual LAN，虚拟局域网）所指的 LAN 特指使用路由器分隔的网络——也就是广播域。使用 VLAN 可以减少在解决移动、添加、修改终端用户等问题时的管理开销；提供控制广播的功能，避免混乱；支持工作组和网络的安全性。对网络进行优化时需根据用户类型和管理功能的不同划分 VLAN，避免混乱。但是如果将 VLAN 设置错的话，也就是直接改变了局域网的拓扑结构，所以在设置 VLAN 时要加倍小心，并应做好相应的关于 VLAN 设置信息的文档的备份等工作。

习题

1. 引起网络故障的原因有哪些?
2. 简述网络故障的排除过程。
3. 简述链路故障的诊断与排错。
4. 简述协议故障的诊断与排错。
5. 简述配置故障的诊断与排错。
6. 简述服务器故障的诊断与排错。
7. 简述拓扑故障的诊断与排错。

实验:网络链路和网络设备故障的诊断与排除

实验目的:

掌握网络链路和网络设备故障的诊断与排除方法。

实验内容:

在网络发生故障时,应识别并排除故障,做好相关的故障记录。

实验步骤:

(1)识别故障现象。
(2)描述故障现象。
(3)列举可能导致发生故障的原因。
(4)缩小故障原因的搜索范围。
(5)隔离并排除故障。
(6)对故障进行分析并记录。

参 考 文 献

1. 王春海，刘晓辉. 网络管理工具实用详解(第 2 版)[M]. 北京：电子工业出版社，2009
2. 刘晓辉. 网络管理工具完全技术宝典[M]. 北京：电子工业出版社，2009
3. 刘晓辉. 网络故障现场处理实践(第 2 版)[M]. 北京：电子工业出版社，2009
4. 刘晓辉. 交换机・路由器・防火墙[M]. 重庆：重庆大学出版社，2008
5. 王淑江. 网络管理[M]. 北京：机械工业出版社，2007
6. 刘晓辉，王淑江. 网络硬件设备完全技术宝典[M]. 北京：中国铁道出版社，2009